X-Pedition™ Security Router

XSR-3020 Getting Started Guide

Version 3.0

P/N 9033866-06

enterasys®

Electrical Hazard: Only qualified personnel should perform installation procedures.

Riesgo Electrico: Solamente personal calificado debe realizar procedimientos de instalacion.

Elektrischer Gefahrenhinweis: Installationen sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

Part Number: 9033866-06 September 2007

Documentation URL: http://www.enterasys.com/support/manuals

Documentacion URL: http://www.enterasys.com/support/manuals

Dokumentation im Internet: http://www.enterasys.com/support/manuals

Regulatory Compliance Information

Federal Communications Commission (FCC) Notice

The XSR complies with Title 47, Part 15, Class A of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: The XSR has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the XSR is operated in a commercial environment. This XSR uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of the XSR in a residential area is likely to cause interference in which case you will be required to correct the interference at your own expense.

WARNING: Modifications or changes made to the XSR, and not approved by Enterasys Networks may void the authority granted by the FCC or other such agency to operate the XSR.

The XSR complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council for Terminal Attachments (ACTA). A label on the circuit board of the Network Interface Module contains, among other information, a product identifier in the format listed in the following table. If requested, this number must be provided to the telephone company.

Product	Product Identifier
NIM-T1/E1-xx, NIM-CT1E1/PRI-xx	US: 5N5DENANET1
NIM-BRI-U-xx	US: 5N5DENANEBU
NIM-ADSL-AC-xx	US: 5N5DL02NEAA
NIM-DIRELAY-xx	US: 5N5DENANEDI
NIM-TE1-xx, NIM-CTE1-PRI-xx	US: 5N5DENANECT

A plug and jack used to connect the XSR to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by ACTA. Refer to the following table and installation instructions for details.

Product	Jack Used
NIM-T1/E1-xx, NIM-CT1E1/PRI-xx, NIM-DIRELAY-xx, NIM-TE1-xx, NIM-CTE1-PRI-xx	RJ48C
NIM-BRI-U-xx	RJ49C
NIM-ADSL-AC-xx	RJ11C

Codes applicable to this equipment:

Product	Facilities Interface Code (FIC)	Service Order Code (SOC)
NIM-T1/E1-xx, NIM-CT1E1/PRI-xx, NIM-DIRELAY-xx, NIM-TE1-xx, NIM-CTE1-PRI-xx	04DU9.BN, 04DU9.DN, 04DU9.1KN, 04DU9.1SN	6.0N
NIM-BRI-U-xx	02IS5	6.0N
NIM-ADSL-AC-xx	02LS2	7.0Y

If the XSR harms the telephone network, the telephone company will notify you in advance that it may need to temporarily discontinue service. But if advance notice is not practical, the telephone company will notify you as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the XSR. If this happens, the telephone company will provide advance notice for you to make necessary modifications and maintain uninterrupted service.

If you experience trouble with the XSR, for repair or warranty information, please contact Enterasys Networks, Inc., at 978-684-1000. If the XSR is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is solved. The XSR is not intended to be repaired by the customer.

Industry Canada Notices

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Equipment Attachments Limitations

"NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas. Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate."

"NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the ringer equivalence Numbers of all the devices does not exceed 5."

R & TTE Directive Declaration

Hereby, Enterasys Networks, Inc. declares that this XSR-1850 X-Pedition Security Router is compliant with essential requirements and other relevant provisions of Directive 1999/5/EC.

Class A ITE Notice

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Clase A. Aviso de ITE

ADVERTENCIA: Este es un producto de Clase A. En un ambiente doméstico este producto puede causar interferencia de radio en cuyo caso puede ser requerido tomar medidas adecuadas.

Klasse A ITE Anmerkung

WARNHINWEIS: Dieses Produkt zählt zur Klasse A (Industriebereich). In Wohnbereichen kann es hierdurch zu Funkstörungen kommen, daher sollten angemessene Vorkehrungen zum Schutz getroffen werden.

Product Safety

This product complies with the following: UL 60950, CSA C22.2 No. 60950, 73/23/EEC, EN 60950, EN 60825, IEC 60950.

Use the XSR with the Advanced Power Solutions (APS61ES-30) power supply included with the branch router. Enterasys Networks strongly recommends that you use only the proper type of power supply cord set for the XSR. It should be a detachable type, UL listed/CSA certified, type SJ or SJT, rated 250 V minimum, 7 amp with grounding-type attachment plug. Maximum length is 15 feet (4.5 meters). The cord set should have the appropriate safety approval for the country in which the equipment will be installed.

Seguridad del Producto

El producto de Enterasys cumple con lo siguiente: UL 60950, CSA C22.2 No. 60950, 73/23/EEC, EN 60950, EN 60825, IEC 60950.

Produktsicherheit

Dieses Produkt entspricht den folgenden Richtlinien: UL 60950, CSA C22.2 No. 60950, 73/23/EEC, EN 60950, EN 60825, IEC 60950.

Electromagnetic Compatibility (EMC)

This product complies with the following: 47 CFR Parts 2 and 15, CSA C108.8, 89/336/EEC, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZS CISPR 22, and VCCI V-3.

Compatibilidad Electromágnetica (EMC)

Este producto de Enterasys cumple con lo siguiente: 47 CFR Partes 2 y 15, CSA C108.8, 89/336/EEC, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZS CISPR 22, VCCI V-3.

Elektro- magnetische Kompatibilität (EMC)

Dieses Produkt entspricht den folgenden Richtlinien: 47 CFR Parts 2 and 15, CSA C108.8, 89/336/EEC, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZS CISPR 22, VCCI V-3.

Hazardous Substances

This product complies with the requirements of European Directive, 2002/95/EC, Restriction of Hazardous Substances (RoHS) in Electrical and Electronic Equipment.

European Waste Electrical and Electronic Equipment (WEEE) Notice

In accordance with Directive 2002/96/EC of the European Parliament on waste electrical and electronic equipment (WEEE):

1. The symbol above indicates that separate collection of electrical and electronic equipment is required and that this product was placed on the European market after August 13, 2005, the date of enforcement for Directive 2002/96/EC.
2. When this product has reached the end of its serviceable life, it cannot be disposed of as unsorted municipal waste. It must be collected and treated separately.
3. It has been determined by the European Parliament that there are potential negative effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment.
4. It is the users' responsibility to utilize the available collection system to ensure WEEE is properly treated.

   For information about the available collection system, please go to www.enterasys.com/services/support/ or contact Enterasys Customer Support at 353 61 705586 (Ireland).

产品说明书附件
Supplement to Product Instructions

部件名称 (Parts)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 (Metal Parts)	×	○	○	×	○	○
电路模块 (Circuit Modules)	×	○	○	×	○	○
电缆及电缆组件 (Cables & Cable Assemblies)	×	○	○	×	○	○
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	×
电路开关 (Circuit Breakers)	○	○	×	×	○	○

○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。
Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363-2006 standard.

×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006 标准规定的限量要求。
Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363-2006 standard.

对销售之日的所售产品, 本表显示,
凯创供应链的电子信息产品可能包含这些物质。注意:在所售产品中可能会也可能不会含有所有所列的部件。
This table shows where these substances may be found in the supply chain of Enterasys' electronic information products, as of the date of sale of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

除非另外特别的标注, 此标志为针对所涉及产品的环保使用期标志. 某些零部件会有一个不同的环保使用期(例如, 电池单元模块)贴在其产品上.
此环保使用期限只适用于产品是在产品手册中所规定的条件下工作.
The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain parts may have a different EFUP (for example, battery modules) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

VCCI Notice

This is a class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI) V-3. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI EMC Statement — Taiwan

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種請況下，使用者會被要求採取某些適當的對策。

Declaration of Conformity

Application of Council Directive(s):	**89/336/EEC** **73/23/EEC**
Manufacturer's Name:	**Enterasys Networks, Inc.**
Manufacturer's Address:	**50 Minuteman Road** **Andover, MA 01810** **USA**
European Representative Address:	**Enterasys Networks, Ltd.** **Nexus House, Newbury Business Park** **London Road, Newbury** **Berkshire RG14 2PZ, England**
Conformance to Directive(s)/Product Standards:	**EC Directive 89/336/EEC** **EN 55022** **EN 61000-3-2** **EN 61000-3-3** **EN 55024** **EC Directive 73/23/EEC** **EN 60950** **EN 60825**
Equipment Type/Environment:	**Networking Equipment, for use in a Commercial or Light Industrial Environment.**

Enterasys Networks, Inc. declares that the equipment packaged with this notice conforms to the above directives.

Australian Telecom

N826

WARNING: Do not install phone line connections during an electrical storm.

WARNING: Do not connect phone line until the interface has been configured through local management. The service provider may shut off service if an un-configured interface is connected to the phone lines.

WARNING: The NIM-BRI-ST cannot be connected directly to outside lines. An approved channel service unit (CSU) must be used for connection to the ISDN network. In some areas this CSU is supplied by the network provider and in others it must be supplied by the user. Contact your service provider for details.

Federal Information Processing Standard (FIPS) Certification

The XSR has been submitted to the National Institute of Standards and Technology (NIST) for FIPS 140-2 certification and is now officially listed on the NIST pre-validation list. For more information about the FIPS validation program, go to http://csrc.nist.gov/cryptval/preval.htm. For the FIPS 140-1 and 140-2 Pre-Validation List, click on the **[PDF]** link at the top of the page.

Independent Communications Authority of South Africa

This product complies with the terms of the provisions of section 54(1) of the Telecommunications Act (Act 103 of 1996) and the Telecommunications Regulation prescribed under the Post Office Act (Act 44 of 1958).

ICASA TE-2002/195 APPROVED

ICASA TE-2002/190 APPROVED

ICASA TE-2003/112 APPROVED

ICASA TE-2003/113 APPROVED

ICASA SS/366.01 APPROVED

VPN Consortium Interoperability

The VPN Consortium's (VPNC) testing program is an important source for certification of conformance to IPSec standards. With rigorous interoperability testing, the VPNC logo program provides IPSec users even more assurance that the XSR will interoperate in typical business environments. VPNC is the only major IPSec testing organization that shows both proof of interoperability as well as the steps taken so that you can reproduce the tests.

VPNC CERTIFIED Basic Interop

VPNC Virtual Private Network Consortium

VPNC CERTIFIED Basic Conformance

Enterasys Networks, Inc. Firmware License Agreement

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between the end user ("You") and Enterasys Networks, Inc., on behalf of itself and its Affiliates (as hereinafter defined) ("Enterasys") that sets forth Your rights and obligations with respect to the Enterasys software program/firmware (including any accompanying documentation, hardware or media) ("Program") in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. "Affiliate" means any person, partnership, corporation, limited liability company, other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, "YOU" AND "YOUR" SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (978) 684-1000.

You and Enterasys agree as follows:

1. **LICENSE.** You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.

2. **RESTRICTIONS.** Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:

   (a) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys' applicable fee.

   (b) Incorporate the Program in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.

   (c) Publish, disclose, copy reproduce or transmit the Program, in whole or in part.

   (d) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.

   (e) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.

3. **APPLICABLE LAW.** This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the Commonwealth of Massachusetts without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Commonwealth of Massachusetts courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

4. **EXPORT RESTRICTIONS.** You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Section 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Cambodia, Cuba, Georgia, Iraq, Kazakhstan, Laos, Libya, Macau, Moldova, Mongolia, North Korea, the People's Republic of China, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

6. **DISCLAIMER OF WARRANTY.** EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY ENTERASYS, ENTERASYS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

7. **LIMITATION OF LIABILITY.** IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

8. **AUDIT RIGHTS.** You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys, and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

9. **OWNERSHIP.** This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

10. **ENFORCEMENT.** You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

11. **ASSIGNMENT.** You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity which acquires substantially all of Your stock assets. Enterasys may assign this Agreement in its sole discretion. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

12. **WAIVER.** A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

13. **SEVERABILITY.** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality, or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

14. **TERMINATION.** Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

Contents

About This Guide

This guide provides a general overview of the XSR-3020 hardware and software features and describes how to quickly install and configure the XSR. Refer to the *XSR CLI Reference Guide* and *XSR User's Guide* for information not contained in this document.

This guide is written for administrators who want to configure the X-Pedition Security Router or experienced users who are knowledgeable of basic networking principles.

This chapter details the following:

- Contents of the Guide
- Conventions Used in This Guide
- Getting Help

Contents of the Guide

Information in this guide is arranged as follows:

- *Chapter 1, Overview,* introduces key features of the XSR and briefly describes hardware installation.
- *Chapter 2, Hardware Installation*, provides a checklist to verify your shipment and describes how to install XSR hardware including NIM and optional CompactFlash cards, and rack-mounting brackets.
- *Chapter 3, Software Configuration,* describes how to initiate and quickly configure the XSR. It also details how to add an interface and subnet mask; set passwords, SNMP, DNS and SYSLOG server values; configure the firewall feature set, upgrade system image and Boot PROM software; consult system statistics, and save configuration changes.
- *Appendix A, Specifications*, outlines hardware specifications including information about: the processor, interfaces, system memory, chassis, power supply, interfaces, required cabling and other accessories, pinout assignments for WAN and LAN interfaces, and LED behavior.

Conventions Used in This Guide

The following conventions are used in this guide:

Note: Calls the reader's attention to any item of information that may be of special importance.

Nota: Llama la atencion del lector a cierta información que puede ser de especial importancia.

Caution: Contains information essential to avoid damage to the equipment.

Precaución: Contiene información esencial para prevenir dañar el equipo.

Achtung: Verweißt auf wichtige Informationen zum Schutz gegen Beschädigungen.

Electrical Hazard: Warns against an action that could result in personal injury or death due to an electrical hazard.

Riesgo Electrico: Advierte contra una acción que pudiera resultar en lesión corporal o la muerte debido a un riesgo eléctrico.

Elektrischer Gefahrenhinweis: Installationen sollten nur durch ausgebildetes und qualifiziertes. Personal vorgenommen werden.

Warning: Warns against an action that could result in personal injury or death.

Advertencia: Advierte contra una acción que pudiera resultar en lesión corporal o la muerte.

Warnhinweis: Warnung vor Handlungen, die zu Verletzung von Personen oder gar Todesfällen führen können!

Bold/En negrilla	Text in boldface indicates values you type using the keyboard or select using the mouse (for example, a:\setup). Default settings may also appear in bold. El texto en negrilla indica valores que usted introduce con el teclado o que selecciona con el mouse (por ejemplo, a:\setup). Las configuraciones default pueden también aparecer en en negrilla.
Italics/It áli ca	Text in italics indicates a variable, important new term, or the title of a manual. El texto en itálica indica un valor variable, un importante nuevo término, o el título de un manual.
SMALL CAPS/ MAYUSCULAS	Small caps specify the keys to press on the keyboard; a plus sign (+) between keys indicates that you must press the keys simultaneously (for example, CTRL+ALT+DEL). Las mayusculas indican las teclas a oprimir en el teclado; un signo de más (+) entre las teclas indica que usted debe presionar las teclas simultáneamente (por ejemplo, CTRL+ALT+DEL).
`Courier font/` `Tipo de letra Courier`	Text in this font denotes a file name or directory. El texto en este tipo de letra denota un nombre de archivo o de directorio.
+	Points to text describing CLI command. Apunta al texto que describe un comando de CLI.
FastEthernet	FastEthernet and GigabitEthernet references are generally interchangeable throughout this guide. Las referencias a los terminos FastEthernet y GigabitEthernet son generalmente intercambiables en el contenido de esta guia.

Getting Help

For additional support related to the XSR, contact Enterasys Networks using one of the following methods:

World Wide Web	www.enterasys.com/support/
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000 To find the Enterasys Networks Support toll-free number in your country: www.enterasys.com/support/
Internet mail	support@enterasys.com To expedite your message, type **[xsr]** in the subject line.
FTP	ftp://ftp.enterasys.com
Login	anonymous
Password	your Email address
Get the latest image and Release Notes	http://www.enterasys.com/download
Additional documentation	http://www.enterasys.com/support/manuals
To send comments concerning this document to the Technical Publications Department: techpubs@enterasys.com Please include the document Part Number in your email message.	

Before contacting Enterasys Networks for technical support, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of any associated Enterasys Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of the problem
- The device history (for example, if you have returned the device before, or if this a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

1

Overview

This chapter introduces the key features of the XSR-3020 and briefly describes hardware installation.

System Description

The XSR is a networking device designed for enterprise regional offices that provides IP routing over GigabitEthernet LAN and T1/E1, Serial (RS232, X.21, V.35, RS422/530, RS449), Dial Services via POTS, ISDN (BRI/PRI) or Frame Relay WAN connections. Virtual Private Network (VPN) support is also provided in Site-to-Site or Remote Access applications.

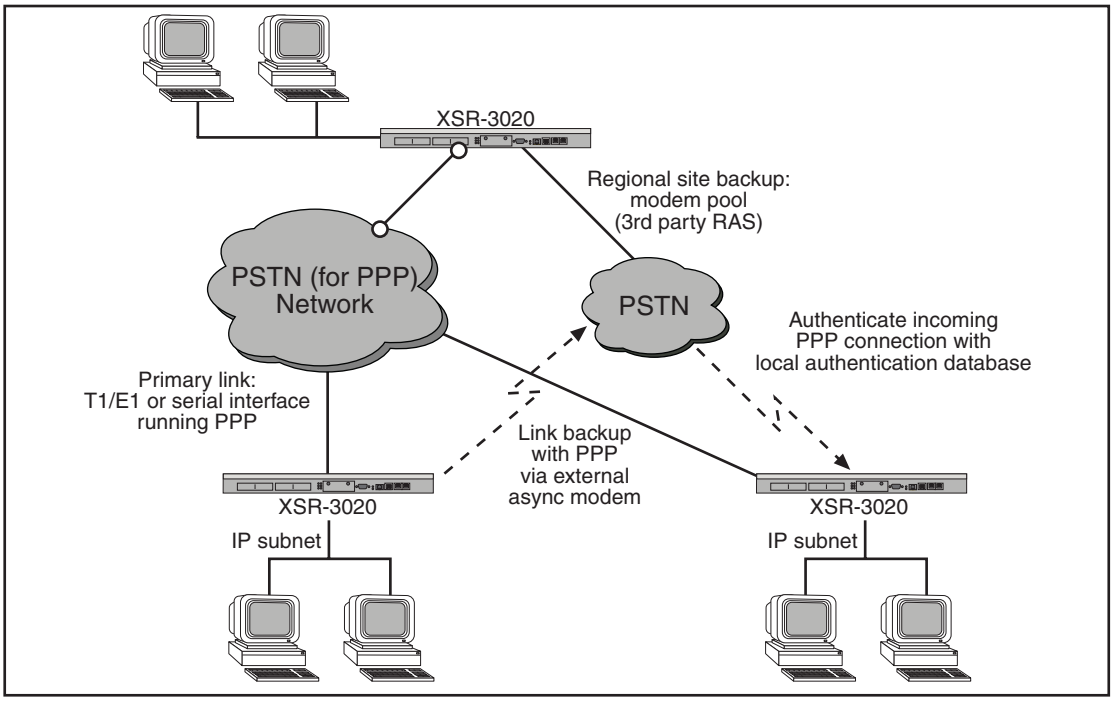
The router can be managed using the Command Line Interface (CLI) and monitored using SNMP v1, v2c/v3 (with standard MIB-II and proprietary MIB support). The XSR also provides Web access to display device data.

The XSR-3020 can be configured to support the following applications:

- *Regional Router* - The XSR serves as a router with multiple WAN link support. It is also capable of providing the same VPN support as the full-featured VPN Gateway for customers who wish to integrate both applications in the same system.
- *Full-Featured VPN Gateway* - The XSR supports up to 1000 simultaneous VPN tunnels at 100 Mbps using 3DES. The VPN Gateway supports the same functionality as the Aurorean Network Gateway series but without local hard disk support.
- *Firewall platform* - The XSR provides a stateful inspection firewall. Processing is performed on the dual MIPS core at 300 Mbps.

A typical deployment of the XSR might be in two branch offices connected to a regional office, as illustrated in Figure 1-1. In this example, one XSR with its associated sub-network has an E1/T1 or high-speed serial WAN connection as its primary link to the Public Service Telephone Network (PSTN) with an asynchronous modem connection in a backup capacity.

Figure 1-1 Typical XSR-3020 Topology

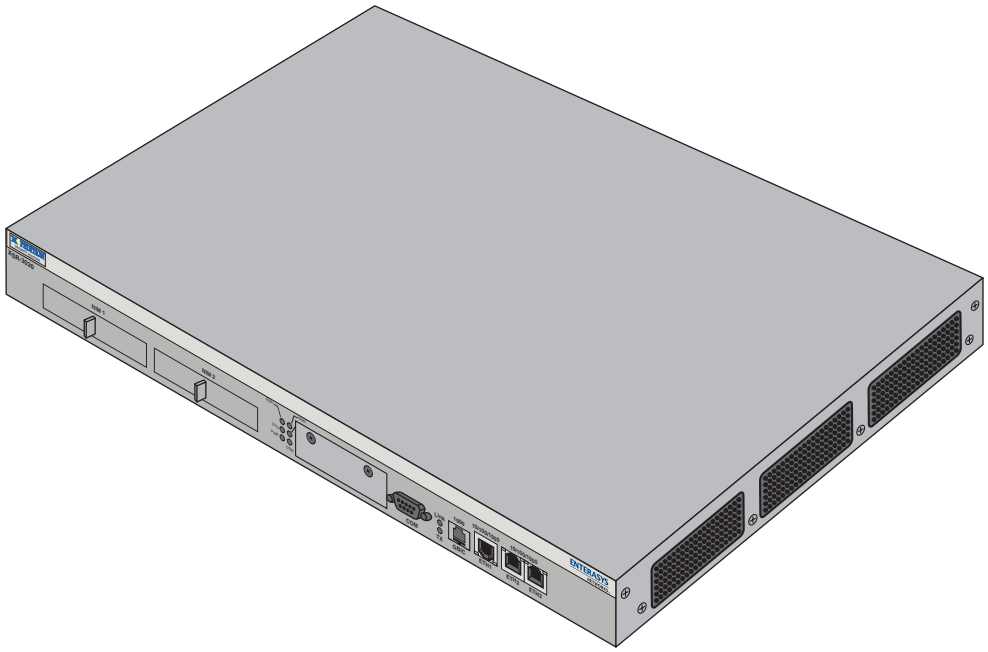


Hardware Features

The semi-modular XSR, shown in Figure 1-2, comes equipped with the following features:

- Standard 1U chassis (1-11/16 inches high by 17 inches wide by 21 inches deep) mountable in a standard 19" rack.
- Broadcom 1250 dual-CPU, 64-bit processor (1700 Dhrystone MIPS @ 600 MHz) with load balancing, 512 KByte on-chip Layer 2 cache, up to two co-issued, load-to-use instruction pairs per cycle, and 32 KByte Instruction and Data caches.
- Internal, universal (100 - 240 VAC) power supply with country-specific line cords.

Figure 1-2 XSR-3020



- Two Network Interface Module (NIM) slots for these optional cards:
  - 1, 2, or 4 full, fractional and channelized T1/E1 WAN NIM with integral CSU/DSU or Primary Rate Interface (PRI) ports (RJ-48C).
  - 1-port T3/E3 channelized/unchannelized WAN NIM with BNC ports. This NIM is also available with up to 16 T1/E1 tributaries and system synchronization of two NIMs.
  - High-speed serial port for up to 230 Kbps asynchronous and 8 Mbps synchronous WAN NIM for leased and dial lines (68-pin serial) with universal connector supporting X.21, V.35, RS422 and EIA530.
  - 1- or 2-port serial Basic Rate Interface (BRI) WAN NIM for S/T (RJ-45) or U ports (RJ-49C).
  - 1-port Annex A (POTS)/C or B (ISDN) ADSL WAN NIMs with RJ-11 connector with CompactFlash card.
  - 2-port T1/E1 Drop and Insert WAN NIM with RJ-45 connectors.
  - 1-port Copper or Fiber Ethernet LAN or WAN NIM with an RJ-45 or MT-RJ multi-mode interface.
- Three 10/100/1000BaseT GigabitEthernet LAN connectors and a Mini-Gigabit Interface Converter (MGBIC) fiber-optic port capable of operating in full or half-duplex modes.
- COM (console) serial interface including modem control signals for remote debugging, or out-of-band configuration
- 128 MBytes of 64-bit, 133 MHz SDRAM/DIMM memory, 8 MBytes of Onboard Flash RAM, optional 16 MByte plug-in CompactFlash RAM card upgradeable to 1 GByte for firmware, image and alarm storage.
- PCI-based, Encryption Module hardware accelerator for: encryption/decryption (3DES), Message Digest (MD-5, SHA-1), and public key acceleration.
- Alarm detection, local and remote loopback, and loopback tests.

- 14 diagnostic LEDs to display port, and system status as well as indicate a Flash upgrade in progress.
- Five system fans with failure detection capability and three fans dedicated to power supply cooling.

Software Features

The XSR provides the following software features:

Operating System

- Multi-threaded OS to fully utilize the XSR's dual processors

Industry-common CLI

- Configuration, performance (status/statistics), and fault (traps/events) management
- Multiple administrators can log into the XSR simultaneously through terminal or remote Telnet/SSHv2 access
- Maximum of five simultaneous Telnet/SSHv2 sessions
- CLI script downloads for bulk configuration
- Alarm/event view and retrieval
- Diagnostic/debug reports and statistics
- Multiple user privilege settings per configuration mode

IP Protocol

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP}
- Transmission Control Protocol/User Datagram Protocol (TCP/UDP)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT) & NAPT
- Dynamic NAT pool based on source and destination
- Dynamic NAT pool with overload
- NAT Port Forwarding
- PAT (NAPT) based on port source and destination
- Telnet & TFTP for device management and configuration
- Debugging tools Ping & TraceRoute
- Secondary IP addressing
- PPP and OSPF debugging
- Internet Group Management Protocol (IGMP)
- Remote Auto Install over Ethernet

- Simple Network Time Protocol (SNTP) server
- OS fallback

IP Routing

- Static and multiple routes to the same destination
- Redistribution of routes from RIP, OSPF, BGP, connected, or static into RIP, OSPF, and BGP
- RIP-1 & RIP-2
- Open Shortest Path First Protocol (OSPF)
- OSPF over Generic Routing Encapsulation (GRE): RFC-2784
- Virtual Router Redundancy Protocol (VRRP)
- Configurable administrative distance (route preference) per protocol for RIP, OSPF and BGP, and per route for static routes
- DNS Proxy (forwarding proxy server)
- Virtual Local Area Networks (VLAN) IEEE 802.1Q
- VLAN Routing including priority support
- Policy Based Routing
- Border Gateway Protocol Version 4 (BGP-4)
- BGP configurable timers and filter tags
- Protocol Independent Multicast - Sparse Mode (PIM-SM)
- Multicast Forwarding over GRE
- Equal-Cost Multi-Path Protocol (ECMP)

SNMP and Statistics Gathering

- Gathering XSR statistics and monitoring using SNMP v1/v2c/v3 using proprietary and standard MIBs including MIB-II Syslog, Configuration Change, TimedReset, Entity, Chassis, Persistence, and Protocol MIBs (OSPF, RIP, FR, and PPP).
- Up/download files to the XSR with the Configuration Management MIB.
- Configure and monitor the XSR using proprietary MIBs: Enterprise VPN and Firewall Configuration, and Host Resources (CPU utilization) via NetSight Atlas Router Services Manager.
- Configuration checksum via MIB
- SNMP Inform support
- Service Level Agreement (SLA) agents
- SNMP-TFTP on-the-fly running configuration
- Hostname in the Syslog message header
- Multiple Syslog servers

Security

- Stateful inspection firewall engine
- FTP, H.323, and RPC (SUN and Microsoft) ALG support
- Application commands for FTP, SMTP, & HTTP
- Firewall logging and authentication
- Firewall interaction with NAT & VPN
- Standard and Extended Access Control Lists
- Denial of Service (DoS) protection
- AAA for firewall, Console, Telnet, SSHv2, PPP and VPN users
- AAA per-interface configuration
- AAA debugging
- Dynamic Firewall configuration
- Onboard URL filtering

PPP

- Sync and asynchronous communications modes accepted
- Authentication of peer entities via Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- IP Address can be assigned from remote device, and the device will support IP address assignment to a remote device. Pools can be configured locally or from a separate server (DHCP).
- Multilink PPP (MLPPP): RFC-1990
- Multi-Class MLPPP: RFC-2686
- Point-to-Point Protocol over Ethernet (PPPoE) and sub-interface monitoring
- Remote Auto Install over PPP

Frame Relay

- DTE support for User Network Interface (UNI) over Frame Relay PVC connections
- 10-bit DLCI addressing using a 2-byte DLCI header
- Per DLCI IP QoS support
- Rate enforcement (CIR) with automatic rate fallback via traffic/adaptive shaping when the network is congested. Automatically restores normal rates when congestion removed
- Congestion control: Backward and Forward Explicit Congestion Notification (BECN/FECN)
- Standard LMIs: ILMI, ANSI Annex D, CCITT Annex A and:
  - *Auto* option for LMI detection/adaptation
  - *None* option for directly connecting XSRs

- Periodic Keep-Alive messages to learn of connection problems
- Multi-protocol interconnect over Frame Relay - RFC-2427
- RFC-2390 Frame Relay Inverse ARP to discover IP address of remote peer when used in multi-point mode and responds to incoming Inverse ARP requests independent of P2P or MP2P
- Multiple logical interfaces over the same physical Frame Relay port: sub-interfaces
- Quality of Service: standard FIFO queuing, or IP QoS on DLCIs.
- Max PDU size of 1600 bytes
- Traffic shaping
- Frame Relay Fragmentation Implementation Agreement (FRF.12)
- Data Communications Equipment (DCE) support
- Frame Relay over ISDN
- Remote Auto Install over Frame Relay

Dynamic Host Configuration Protocol (DHCP)

- Temporary or permanent network (IP) address allocation to clients
- Network configuration parameter assignment to clients
- Persistent storage/database of network values for network clients - Bindings Database
- Persistent storage of network client lease states kept across reboot
- Persistent and user-controllable conflict avoidance to prevent duplicate IP address including configurable ping checking
- Visibility of DHCP network activity and leases through operator reports statistics and logs
- DHCP Client

Integrated Services Digital Network (ISDN) - BRI/PRI

- Circuit Mode Data (CMD): Channels (DS0s) are switched by the CO to the destination user for the duration of the call
- Outgoing calls supported for Backup, DoD/BoD
- Incoming calls routed to the correct protocol stack based on called number/sub-address and calling number/sub-address
- Permanent B-channel support, i.e. 64 or 128 kbps lease line. Each BRI port can be set for CMD or Leased-Line mode of operation
- BRI supported switches: ETSI
- BRI: TEI auto-negotiated
- Q.921/Q.931 (Layer 2/Layer 3) configuration is set automatically by selection of switch type
- PRI supported switches: ETSI, NI, DMS100, NTT
- PRI: Handling restart and maintenance modes automatically set
- PRI: Fixed TEI to 0
- ISDN switched and Leased Line connections

- Bandwidth optimization (BoD) & Dial on Demand (DoD)
- Bandwidth Allocation Protocol (BAP)
- Security: PAP/CHAP
- Call monitoring
- Multilink PPP (MLPPP)
- Per call activation for NTT switches
- Frame Relay over ISDN

Quality of Service (QoS)

- Traffic classification using IP Precedence and DiffServ Code Point (DSCP) bits, and multiple-field (L3, L4 and other headers) inspection. *Match-any* and *match-all* options also define a class-map.
- Priority Queuing or Class-based Weight Fair Queueing (CBWFQ) to specify the policy-map
- Random and Weighted Early Detection (RED/WRED) and Tail Drop congestion avoidance
- QoS over VPN
- QoS on Input

Virtual Private Network (VPN)

- Site-to-Site application
  - 200 tunnels with standard 64-Mbyte DIMM
  - IPSec/IKE with pre-shared secrets
  - IPSec/IKE with Certificates (PKI)
  - EZ-IPsec with PKI or pre-shared secrets:
  - Network Extension Mode (NEM)
  - Client mode
- Remote Access application
  - 200 tunnels with standard 64-Mbyte DIMM installed
  - L2TP/IPSec protocols
  - – Certificate and PKI environment

    MS-ChapV2, EAP user authentication:

    Username/Password (local database & RADIUS)

    SecurID (third-party plug-in)

    Certificates (embedded/smart cards) – Microsoft only
  - – PPTP protocol

    MS-ChapV2, EAP user authentication

    Local Database & RADIUS

SecurID (third-party plug-in)

Certificates (embedded/smart cards) – Microsoft only

- Encryption
  - Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Data Encryption Standard (DES)
  - 3DES/DES acceleration
- Data Integrity
  - MD5 & SHA-1 algorithms
- Internet Protocol Security (IPsec)
  - Encapsulating Security Payload (ESP), Authentication Header (AH) & IPComp
  - Tunnel & Transport mode
  - Diffie-Hellman Groups 1 & 2
  - Mode Config for IP address assignment
  - NAT Traversal via UDP encapsulation
- Public Key Infrastructure (PKI)
  - Microsoft, Verisign Certificate Authority (CA) support
  - Simple Certificate Enrollment Protocol (SCEP)
  - Chained CA support
  - CRL checking (Hypertext Transfer Protocol [HTTP] & Lightweight Directory Access Protocol (LDAP)
- Network Address Translation (NAT)
  - Static NAT, on the interface and port-forwarded static NAT
  - PAT (NAPT) by port source and destination address
  - Dynamic NAT by source/destination IP address
  - Dynamic NAT pool mapping with overload
  - PPTP/GRE ALG and arbitrary IP address for NAPT
  - Multiple NATs on an interface
- Dynamic Host Configuration Protocol (DHCP)
  - DHCP Server
- OSPF over VPN
- DF Bit override

GRE over IPSec

- ToS bit preservation
- IP helper on VPN interfaces
- IETF/Microsoft-compatible NAT traversal for L2TP
- QoS over VPN

Asynchronous Digital Subscriber Line (ADSL)

- POTS and ISDN circuit support
- ATM Frame UNI (FUNI) data framing format
- OAM cells: AIS, RDI, CC, Loopback over F4 and F5 flows
- Up to 30 ATM Permanent Virtual Circuits (PVCs)
- ATM UBR traffic class
- ATM Adaption Layers 0, 5
- PDU encapsulation types:
  - PPP over ATM (PPPoA) (routed)
  - IP over ATM (routed)
  - PPP over Ethernet over ATM (PPPoE) (routed)
- Responds to inverse ARP requests
- Maintenance of SNMP Interface and Interface Stack tables
- Remote Auto Install over ADSL

Dial Service

- Asynchronous serial support through an external modem
- Synchronous serial
- Outbound calling
- Unnumbered Interface Addressing
- PPP encapsulation
- Authentication from XSR's database for PAP & CHAP
- Dialer profile support
- Configurable redialer
- ISDN callback
- Dialer watch
- Dialer interface spoofing
- Incoming call support for analog modems

Dial Backup

- IP Interfaces backup

Dial-on-Demand/Bandwidth-on-Demand (DoD/BoD)

- PPP Point-to-Multipoint & Multi-to-Multipoint connections
- MLPPP Point -to-Multipoint & Multi-to-Multipoint connections
- Incoming Call Mapping connections

- Switched PPP Multilink connections
- Backup using ISDN & MLPPP connections
- Dialer interface spoofing
- Dialer watch

Installation Overview

Installing the XSR consists of performing the following general steps. For detailed instructions, refer to *Chapters 2* and *3* of this manual.

1. Unpack the XSR from the shipping box. Remove accessories.

   Items included in the shipping box are shown in Chapter 2 of this manual. If you are missing any of these items, contact your authorized Enterasys Networks reseller or Enterasys Networks Customer Support as described in the *XSR Quick Start Guide.*

   Cabling is not supplied with the XSR. Refer to page A-2 for part numbers and contact your Enterasys Networks sales representative.
2. Install any optional memory component.
3. Install NIM cards.
4. Mount the XSR in a standard 19" rack.
5. Connect Ethernet cable(s) to the GigabitEthernet LAN port(s).
6. Do one of the following or both:
   - Connect a NIM cable, attaching one end to the RJ-*xx*, BNC or optical port on the XSR and the other to a network connector/hub.
   - Connect the serial cable to the High Speed serial port, attaching one end to the 68-pin, SCSI III type connector on the XSR and the other end to a network device.
   - Connect all other NIM cables.
7. Connect the COM serial cable, attaching the female end to the COM port of the XSR and the other end to the DB-9 serial port on your terminal or PC.
8. Connect the appropriate end of the country-specific power cords to the AC Inlet/ Switches at the back of the XSR and plug the other ends into a wall socket.

Once the XSR is connected, you can begin software configuration, which is described in Chapter 3, Software Configuration.

2

Hardware Installation

Introduction

This chapter provides a checklist to verify your shipment, suggestions for the installation site, and describes how to install the following XSR hardware:

- NIM cards
- Optional - CompactFlash card (standard with ADSL NIM)
- Connecting cables

Note: For instructions on installing a balun and grounding shunt/terminal strip on E1 NIM cards only, refer to *Appendix A: Specifications* on page 1.

Verifying Your Shipment

Before installing the XSR, first check your shipment to ensure that everything you ordered arrived safely. Open the shipping box(es) and verify that you received the following equipment:

- XSR chassis with installed hardware including any optional NIM cards (shipped separately)
- One country-specific power cable
- One console (COM) cable
- Rack mount assembly
- Quick Start Guide

Installation Site Suggestions

When determining an installation site for the XSR chassis, follow the guidelines outlined below:

- For proper cooling, maintain a minimum clearance of 15.2 centimeters (6 inches) behind the chassis and 5.08 centimeters (2 inches) of clearance on either side of the chassis.
- If installing the XSR chassis as a free-standing unit on a shelf, ensure that the shelf can support a minimum weight of approximately 17 pounds per fully loaded chassis plus the weight of the connected network cables.
- For access to the rear of the chassis, allow an area of 48.26 centimeters (19 inches) wide by 61 centimeters (24 inches) deep.
- If installing the XSR chassis in an equipment rack, ensure that the rack can support and remain stable with the chassis installed.

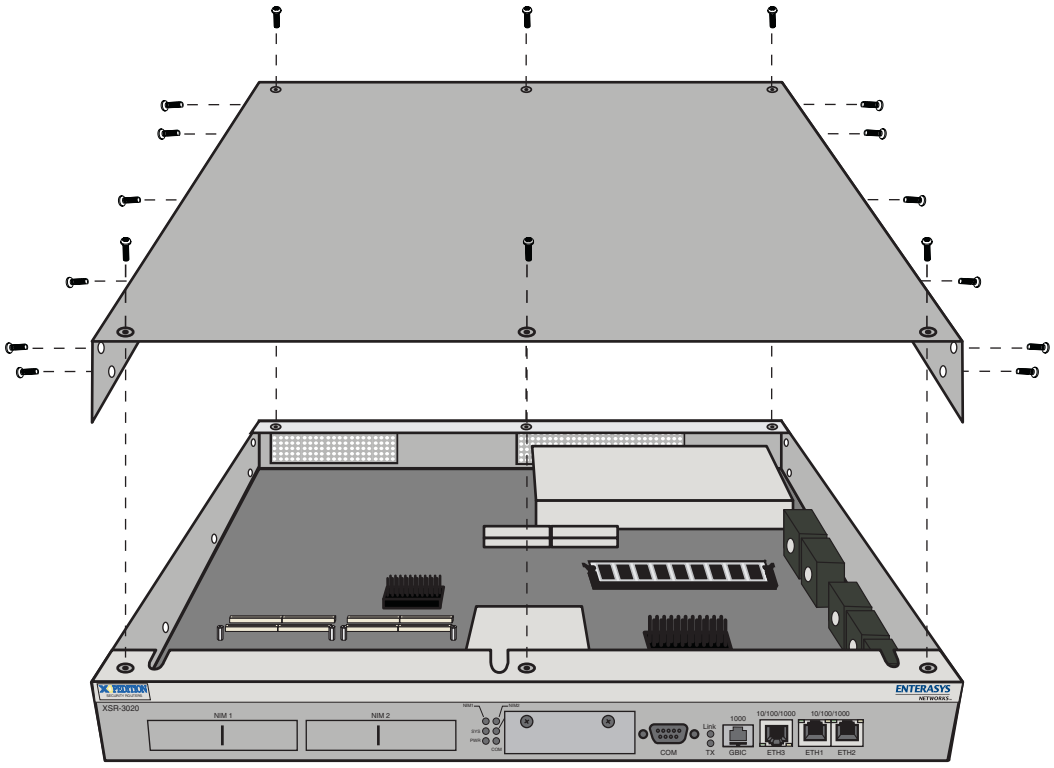
- Each XSR AC power supply requires a three-pronged power receptacle capable of delivering the current and voltage specified in *Appendix A*. An AC outlet on a separately fused circuit is required for each XSR to provide power redundancy, and must be located within 182 centimeters (6 feet) from the site. The power cord used and type of outlet is dependent on the country. In the United States, a power cord with a NEMA 5-15P plug is provided with each XSR.
- Ambient temperature at the installation site must be maintained between 0° and 40°C (41° to 104°F). Temperature changes must be maintained within 10°C (18°F) per hour.

Installing NIM Cards and Rack Mounting

Perform the following steps to install optional NIM card(s) and rack mount the XSR:

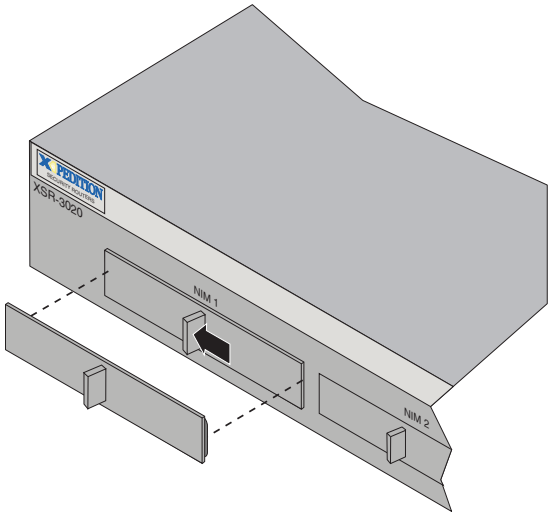
1. Be sure the power cord is disconnected before you add a NIM card.
2. Place the XSR on a flat, static-free surface.
3. Remove the XSR cover from the chassis, as shown in Figure 2-1, by first removing screws from the sides and top.

Figure 2-1 Removing XSR Cover



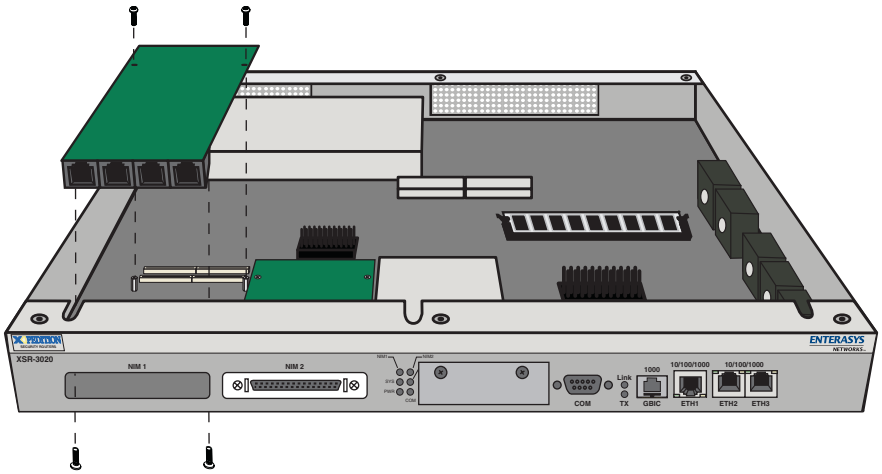
4. Remove the NIM slot cover, as shown in Figure 2-2, by grasping the handle and pulling it to the side before taking it out.

Figure 2-2 Removing NIM Slot Cover



5. Gently attach the NIM card(s) to the connector on the motherboard and secure with four screws, as shown in Figure 2-3.

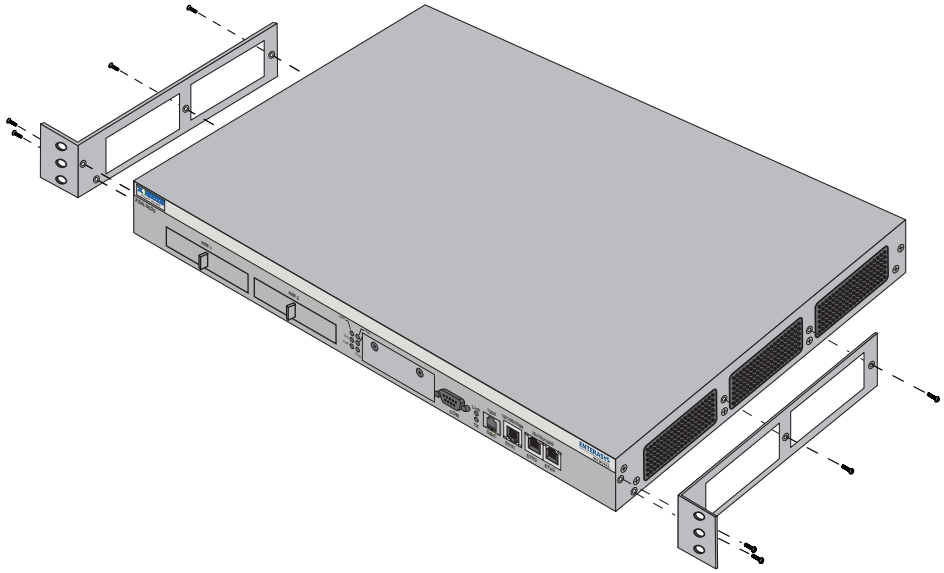
Figure 2-3 Attaching NIM card to Motherboard



6. Re-install the chassis cover.

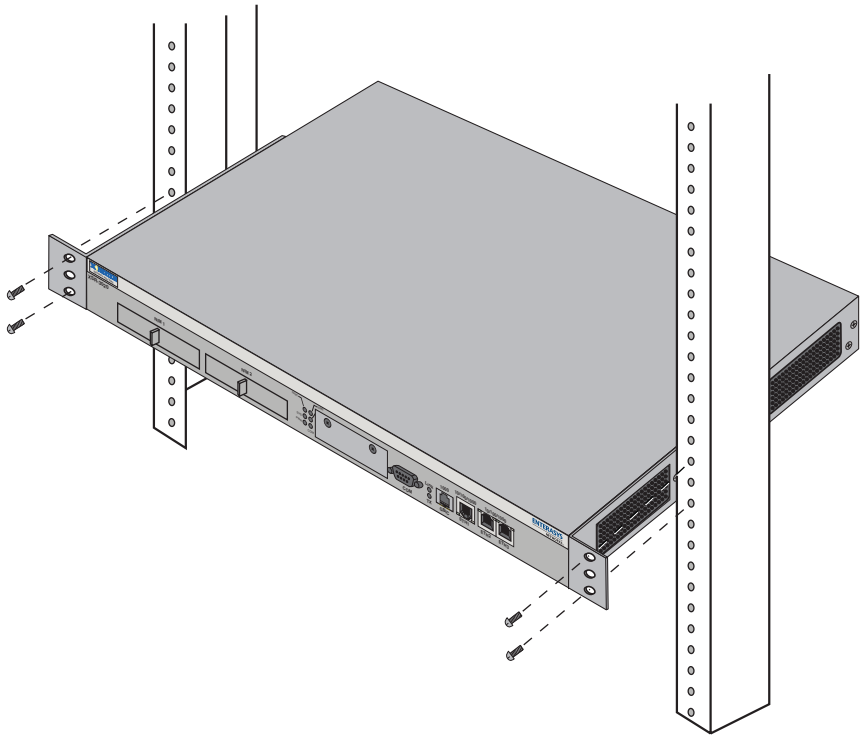
7. Attach the rack brackets to the chassis with the screws supplied, as shown in Figure 2-4.

Figure 2-4 Fastening Rack Brackets



8. Mount the bracketed XSR to your rack, as shown in Figure 2-5.

Figure 2-5 Attaching XSR to Rack



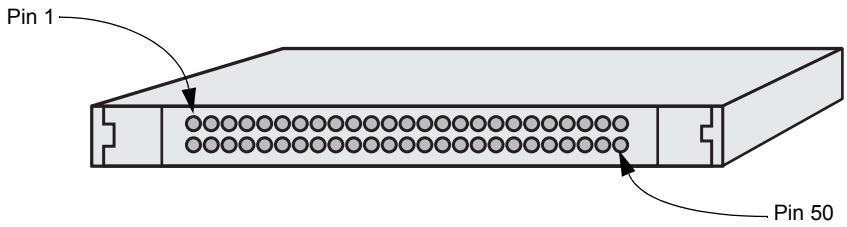
Installing a CompactFlash Memory Card

An optional CompactFlash (CF) memory card provides additional non-volatile storage capabilities in various increments. The CF's controller interfaces with a host system allowing data to be written to and read from the CF's flash memory module. The XSR supports Type I and II CompactFlash card types. Refer to Figure 2-6 for a generic illustration of the card.

The CF's memory is large enough to store image files. You can do so simply by using the Bootrom Monitor mode **copy** command. For example, to copy a file from the Onboard *flash:* directory to the *cflash:* directory while in the *flash:* directory, enter:

```
XSR>copy <source_name> cflash:<destination_name>
```

Figure 2-6 Typical CompactFlash Card

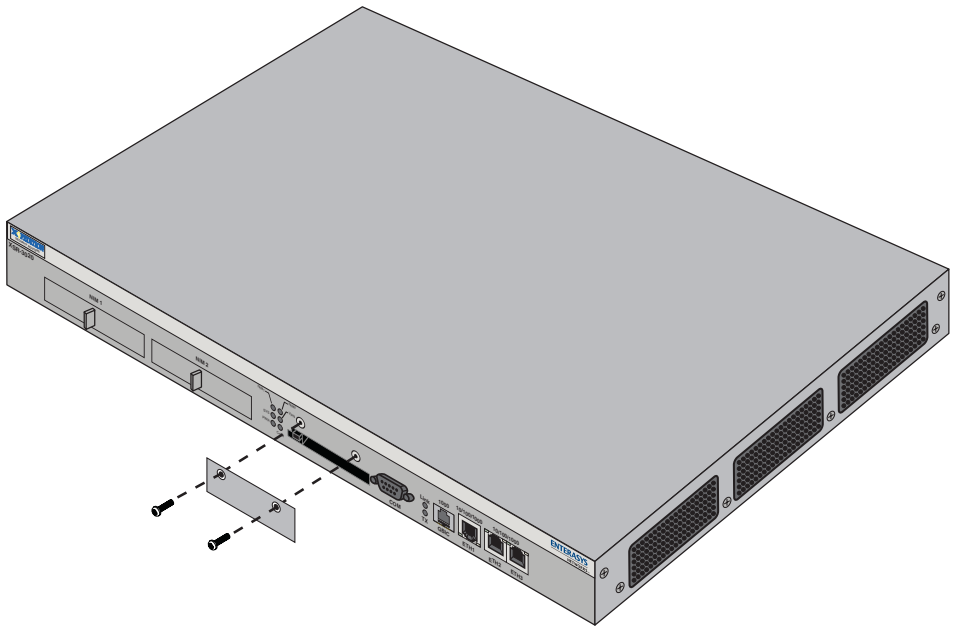


CompactFlash Card Installation

Follow the steps below to install the CompactFlash card:

1. If your CF is already formatted, first remove the cover plate as shown in Figure 2-7. If it is not formatted, jump to "Formatting the CompactFlash Card" on page 2-6.

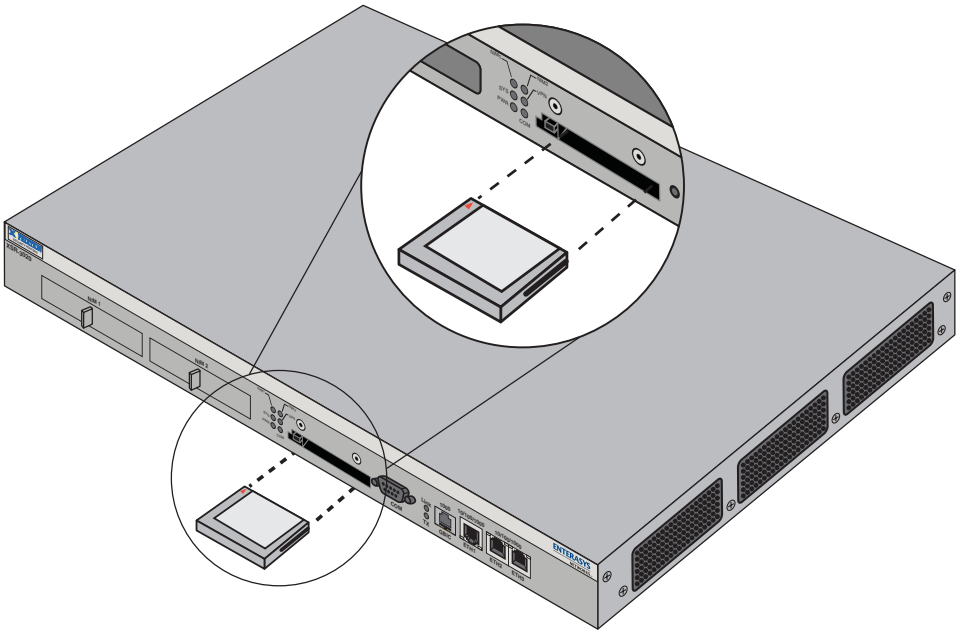
Figure 2-7 Removing CompactFlash Cover Plate



2. Seat the card in the PCMCIA interface as shown in Figure 2-8.

   Gently insert the CF into the slot, taking care that the CF's wider grooved edge fits into the wider track of the PCMCIA interface. If the card does not seat easily but stops halfway into the slot, do not force it in - the card was inserted incorrectly. Flip it over and re-insert. Note that the XSR's CF eject mechanism pops out for easy removal when you install the card. Also, you can re-attach the cover after the CF card is installed for added security.

Figure 2-8 Installing CompactFlash Card



CompactFlash Card for the ADSL NIM

The ADSL NIM is shipped with a CompactFlash card carrying the DSP firmware necessary for connecting to a DSAM. Refer to Figure 2-13 for an illustration and installation instructions.

Formatting the CompactFlash Card

If your CF is *not* formatted, there are two ways you can format the card:

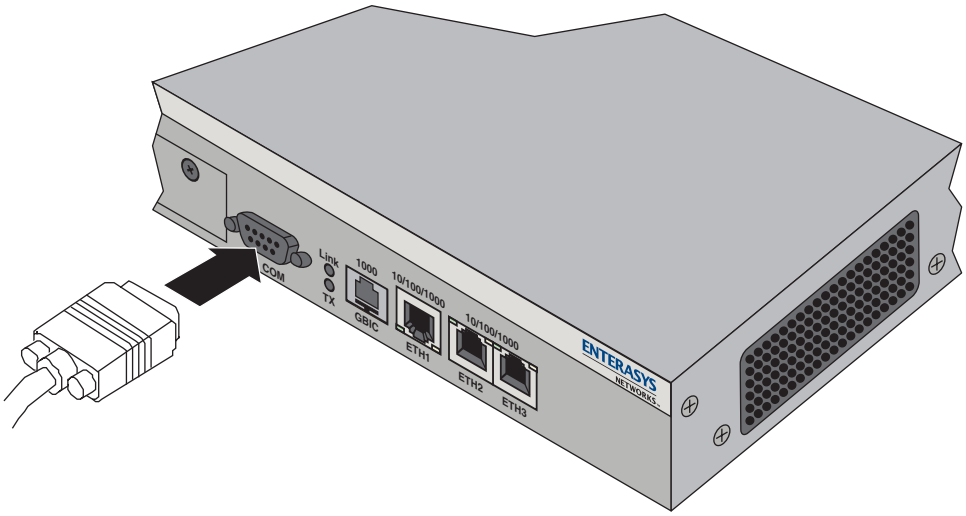
- Use the XSR Bootrom Monitor Mode **`ffc`** command. A few seconds after you boot up the XSR, press the CTRL-C keys and a password prompt will appear. Press ENTER (factory default) if you have not defined any password. The Bootrom Monitor Mode will appear. Enter **`ffc`** and the router will complete the formatting.
- Install the CF in a PCMCIA card and enter the Windows format command. For further instructions, refer to Windows documentation.
- After completing CF formatting via Bootrom Monitor Mode, use the **`bc`** command to restart the XSR in normal mode.

Connecting Cables

Perform any of the following steps to connect your cabling to optional WAN or LAN NIMs, GigabitEthernet ports, and power supply:

1. Connect the serial COM cable provided in the packing box to your PC connector, as shown in Figure 2-9.

Figure 2-9 Connecting Serial COM (Console) Cable



2. Connect WAN cables to the T1/PRI or BRI port(s), or High Speed Serial, T3/E3, ADSL, or T1 Drop & Insert WAN ports, as shown in Figure 2-10, Figure 2-11, Figure 2-12, Figure 2-13, or Figure 2-14, respectively.

Figure 2-10 Attaching T1/PRI or BRI Port Connector

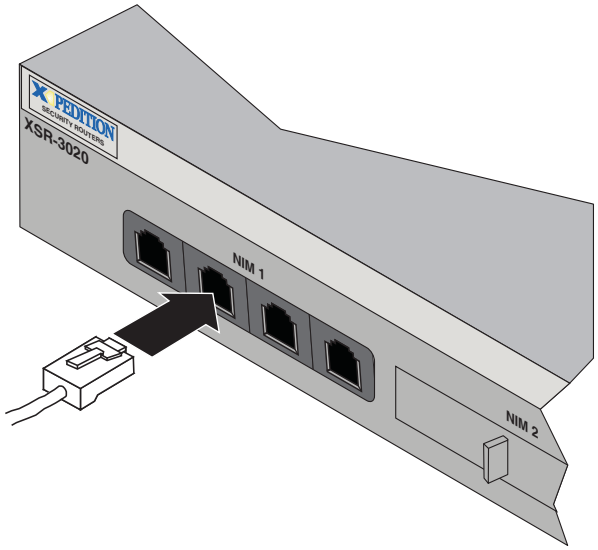


Figure 2-11 Connecting High Speed Serial Connector

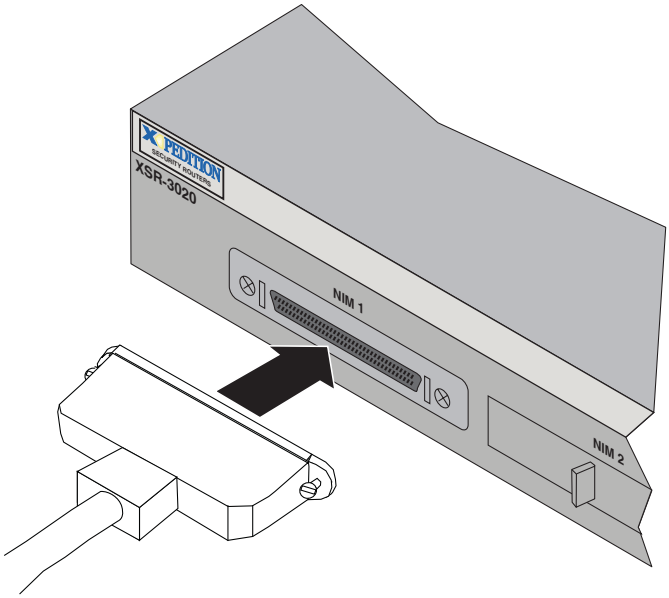


Figure 2-12 Attaching T3/E3 BNC Connectors

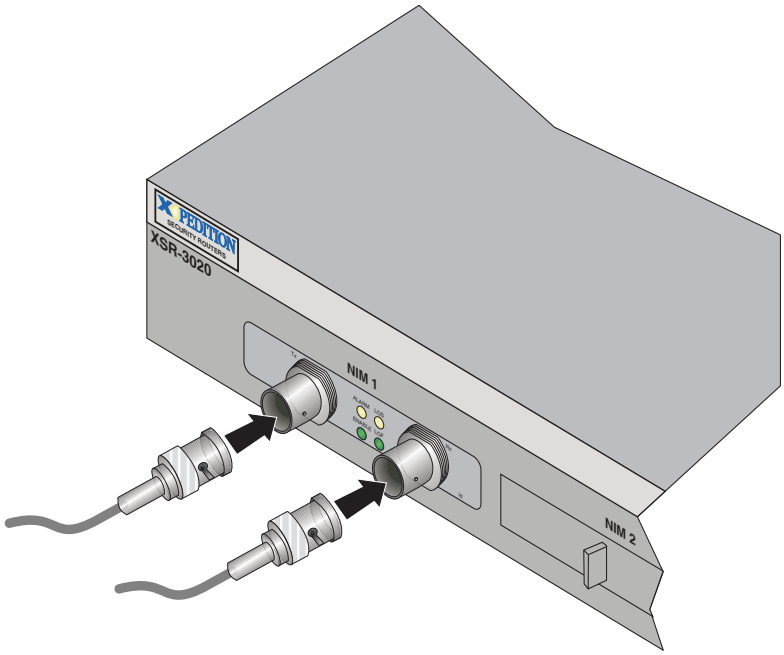
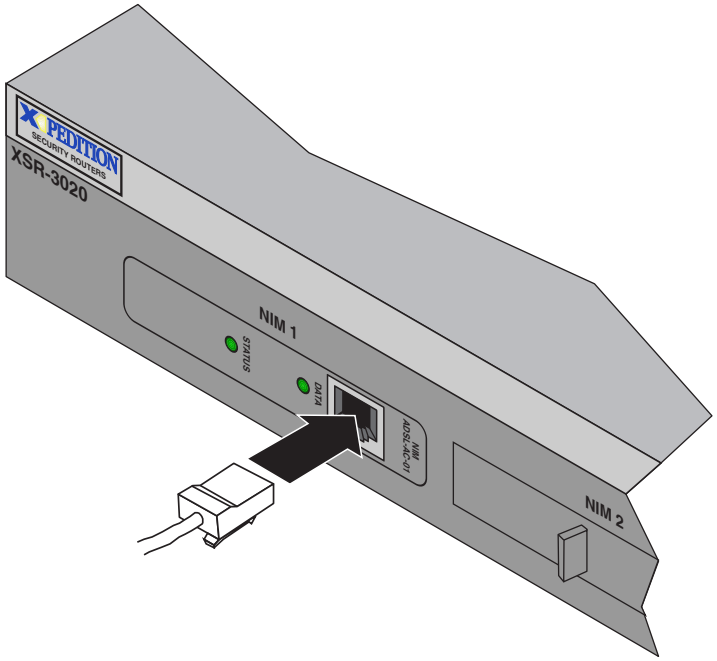


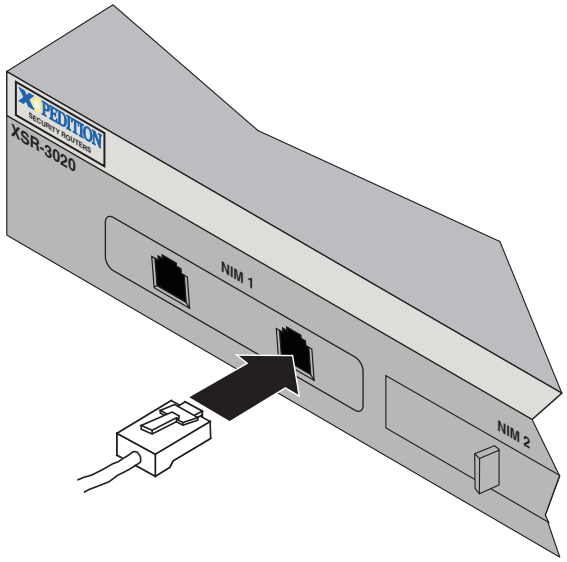
Figure 2-13 Connecting ADSL Connector



A CompactFlash card is provided with the XSR ADSL NIM. It is loaded with the Digital Signal Processing (DSP) firmware (**`adsl.fls`**) required to communicate with your DSLAM. When inserted into the Compact Flash slot - upon first configuring an ATM interface - the XSR's ADSL driver will copy **`adsl.fls`** into host memory where it will remain available for use on demand. Be aware that if all ATM interfaces are deleted, **`adsl.fls`** must be recopied into Flash.

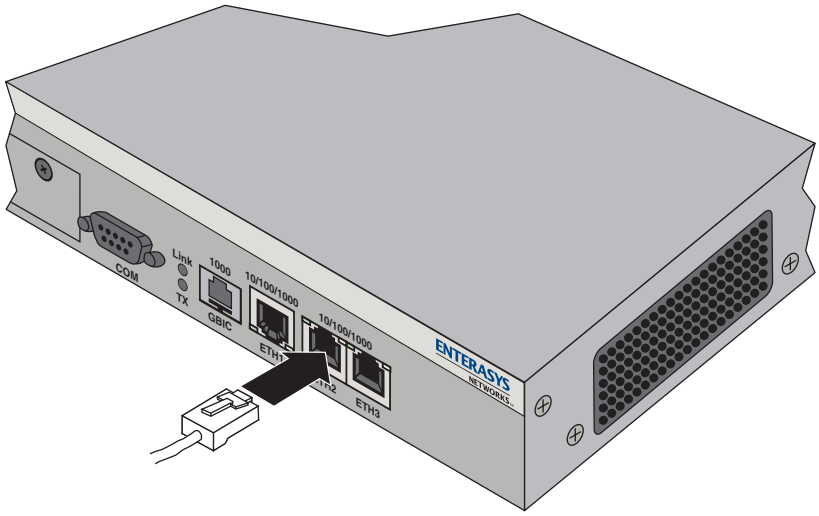
Note: The XSR supports one installed ADSL NIM card type at a time (multiple installed cards must be of the same type).

Figure 2-14 Attaching T1 Drop & Insert Connector



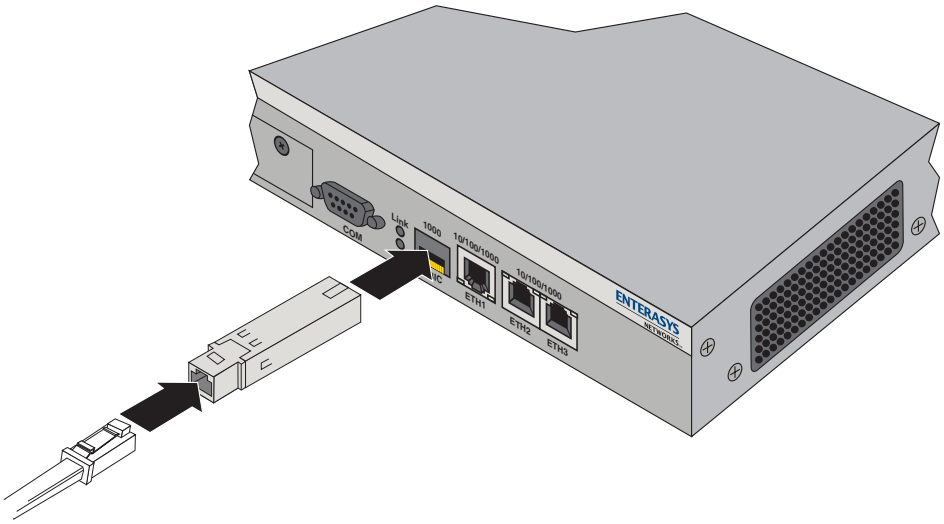
3. Connect the Ethernet port(s) to your LAN connectors with a cable, as shown in Figure 2-15.

Figure 2-15 Attaching Ethernet Connector



4. Insert the Mini-GBIC module in the GBIC slot then connect the optical cable, as shown in Figure 2-16.

Figure 2-16 Inserting Mini-GBIC Module



5. Attach either the Ethernet or Fiber Ethernet LAN NIM, as shown in Figure 2-17 and Figure 2-18, respectively.

Figure 2-17 Attaching Ethernet LAN NIM Connector

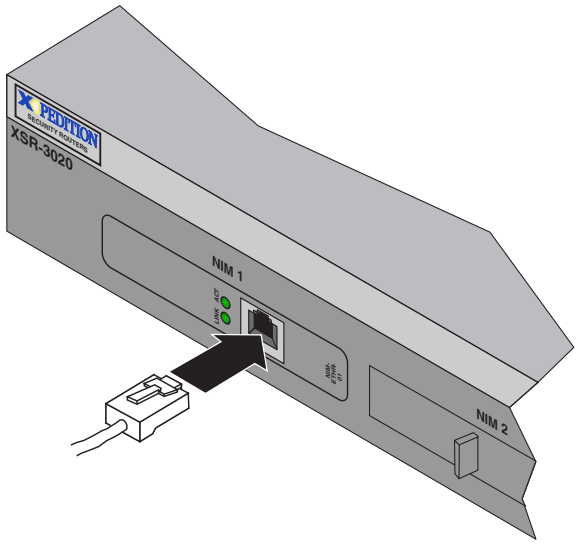
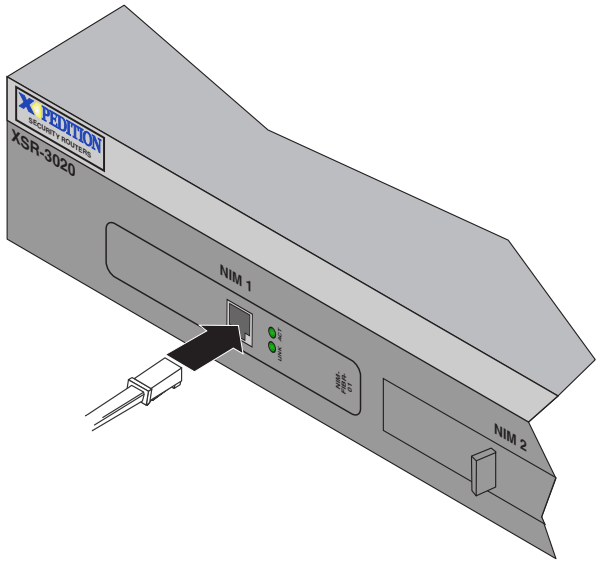
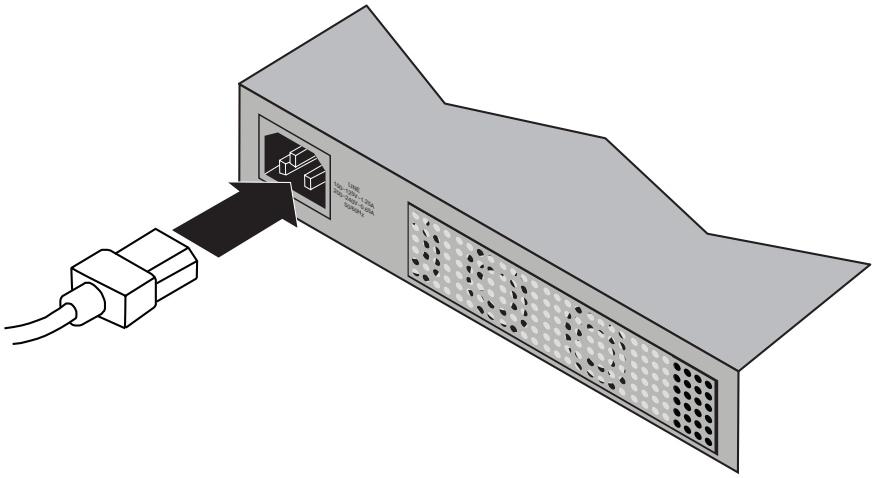


Figure 2-18 Attaching Ethernet Fiber LAN NIM Connector



6. Attach the power supply cord to the connector at the rear of the XSR, as shown in Figure 2-19 and plug in the country-specific power cord connects to a wall socket. The XSR will power up.

Figure 2-19 Connecting Power Supply Cord



You are now ready to configure the software and initialize the XSR. Continue with Chapter 3, Software Configuration.

3

Software Configuration

This chapter describes how to initialize, quickly set up and verify your configuration for the XSR. Refer to the *XSR CLI Reference Guide* for a more thorough explanation of commands and parameter options. The chapter also includes sample configuration scripts, detailed XSR rebooting characteristics and Bootrom Monitor mode instructions.

Software configuration comprises the following procedures:

- Initialize the XSR software
- Open a console (COM) session to the XSR
- Name the XSR and add users/passwords
- Set up LAN ports
- Configure WAN ports for dialer and backup dialer service
- Configure the Firewall feature set
- Configure IP routing: RIP or OSPF
- Configure Frame Relay networks
- Set up a backup line
- Create an SNMP community string and traps
- Configure message logging and severity level
- View your configuration
- Connect via SSH, Telnet or the Web
- LAN/PPP Services Sample Configuration
- Frame Relay WAN Link and PPP Backup Sample Configuration
- VPN configurations (see the *XSR User's Guide* for a Client example)

Initializing XSR Software

1. Be sure the NIM cards are installed and cable connections are snug.
2. After attaching the power cord at the rear of the XSR and powering up the router (as described in Chapter 2) the LED sequence proceeds as follows:
   - Power LED turns ON.
   - All LEDS flash quickly on and off starting from the SYS LED on the left, proceeding to the right.

- ETH 10/100/1000 LEDs turn ON and OFF a few times during initialization as the XSR proceeds from bootrom to power up diagnostics to software image, then they remain ON or OFF depending on the LAN type.
- ETHERNET Activity LEDs blink when frames pass on the LAN.
- COM Activity LED is OFF until the CLI comes up. Then it blinks ON/OFF during console keyboard input or output.
- NIM LEDs are OFF until the CLI comes up. Then they are turned ON if a supported card is present (T1/E1 or Serial), *and* the card passes the power-up diagnostics test.

3. XSR software initializes in two phases. A cold start (including power cycling) is marked by diagnostic and router software phases. A warm start skips the powerup diagnostics and boots to router software. First-time startup is a cold start with the following sequence of events:

- Basic hardware initialization of the processor, memory, and other components occurs.
- Bootrom Monitor mode is accessible now and can be entered by pressing a special key combination within a 5-second interval. For more information, refer to "Bootrom Monitor Mode Commands" on page 3-35.
- Power-up diagnostics test the following hardware blocks:
  - RAM size is detected
  - On-board Flash size is detected
  - GigabitEthernet is checked
  - Ethernet on motherboard is checked
  - NIM cards 1 and 2 is checked
  - Real-Time Clock are checked
  - Front panel LEDs are set to reflect current status
- Diagnostics test results are saved for later use by system software.
- The software image in Flash memory is verified by checksum.
  - If no valid image exists in **`flash:`** or **`cflash:`**, Bootrom Monitor mode is acquired.
  - If the default file (*xsr3000.fls*) is not found as specified in Bootrom mode, an FTP/TFTP server as defined in network parameters of Bootrom mode is queried.
  - If the image is not found remotely, initialization is suspended in Bootrom mode.

Note: Optionally, you can create a *boot-config* file to identify the name of a firmware file from which the XSR boots. Refer to the **boot system** command in the *XSR CLI Reference Guide* for more information.

- A valid image in Flash memory, if present, is decompressed.
- The decompressed software image is loaded into RAM.
- Execution is passed to the software image.
- The operating system is started.
- The Flash startup configuration files (*startup-config*, *private-config*) become the running configuration.
- All software modules are initialized. If an error occurs when processing *startup-config*, the CLI will continue processing the file until the end. If the file contains more than one error, only the

first error will be reported, along with a count of the sum of errors incurred. In the case of a single error, only the error line will be reported. Error messages will be logged as well. Because the result of continuing to process a flawed *startup-config* is not predictable, the nature and position of the syntax error may cause the erroneous configuration of the XSR.

- Router ports and protocol stacks are initialized based on startup configuration.
- Alarms and messages reported during initialization are logged.
- COM is up.
- The XSR is up.

To view the screen output produced when the XSR reboots, refer to "XSR Rebooting Characteristics" on page 3-32.

Opening a COM (Console) Session

1. Open a COM (console) session to the XSR using a communications program.

   Set the session properties as follows: BPS - 9600, Data bits - 8, Parity - none, Stop bits - 1, Flow control - none. Refer to "Initialization Output" on page 3-32 to view XSR initialization data.

2. When the XSR login appears, enter **admin** and enter no (blank) password. Note that logins and passwords can be changed later.

Note: You can abort RAI at any time by pressing any key.

Refer to the following section for quick configuration of RAI. For a full description of RAI including how it works, refer to "Chapter 2: Managing the XSR" in the *XSR User's Guide*.

Optional: Configuring Remote Auto Install

In short, the RAI application transports a startup configuration file from a TFTP server for use in configuring the remote XSR. This file is placed in the **`Flash:`** directory as the **`startup-config`** and executed via the normal startup process. RAI is supported on a Frame Relay network running on a serial NIM card (configuration example shown below), RAI over Ethernet (with DHCP), RAI PPP over a Leased line or RAI over an ADSL network.

For remote XSR setup, you need only hook up cabling as described in *"Chapter 2: Hardware Installation"* of this guide.

Configuring RAI for Frame Relay

To configure two remote XSRs with RAI over Frame Relay, perform the following setup on the central site. On multi-point Serial sub-interface 1/0.1, configure DLCIs 16 and 18 to *statically* map to IP addresses 133.133.1.2 and 133.133.1.3. If the DLCI will onnect to a remote XSR running RAI, then add the *bootp* parameter after the static IP address.

This configuration supports two remote XSRs connected on DLCIs 16 and 18. Make sure with your Frame Relay provider that these DLCIs terminate at the location of the remote XSRs. To add more remote XSRs, you will need additional DLCIs.

Note the use of a *helper-address* to specify a destination address for UDP broadcasts and forward traffic to the DNS and TFTP servers. In the example below, DNS and TFTP servers reside on the

same node - 10.10.1.2 (configuration of DNS and TFTP servers are not shown here). In short, the DNS server should map IP addresses 133.133.1.2 and 133.133.1.3 to hostnames. On the TFTP server, you should create a startup-config file with names <hostname>-config in a directory accessible by TFTP.

```
XSR(config)#interface serial 1/0.1 multi-point
XSR(config-if<S1/0.1>)#ip helper-address 10.10.1.2
XSR(config-if<S1/0.1>)#ip address 133.133.1.1
XSR(config-if<S1/0.1>)#frame-relay interface-dlci 16 ip 133.133.1.2 bootp
XSR(config-if<S1/0.1>)#frame-relay interface-dlci 18 ip 133.133.1.3 bootp
XSR(config-if<S1/0.1>)#no shutdown
XSR(config-if<S1/0.1>)#exit
XSR(config)exit
XSR#copy running-config startup-config
```

RAI displays the following phased output on the remote node. Refer to the accompanying notes for additional explanation of phases.

```
********************* REMOTE AUTO INSTALL STARTING ***************
```

+ *RAI is starting up.*

```
************* REMOTE AUTO INSTALL ATTEMPTING FOREVER **************
```

+ *Persistent (or Non-Persistent) RAI is attempted.*

```
Phase 0 - Initialization and Starting search for proper media-type
Phase 0 - Trying media-type V35
******** PRESS ANY KEY TO TERMINATE REMOTE AUTO INSTALL ***********
```

+ *A periodic reminder that you can terminate the program at any time by depressing any key on your keyboard. Be aware that any existing startup-config that may exist in the node will be executed.*

```
Phase 1 - Trying media-type RS232
```

+ *Upon failing, the next media-type is tried.*

```
Phase 1 - Frame Relay interface Serial 1/0 reported DLCI 16 active
```

+ *Frame Relay has successfully found a FR network with active DLCIs.*

```
Phase 2 - transmitting bootp - attempt #1
```

+ *The bootp client is sending out a request. At most, five requests will be tried.*

```
Phase 3 - received IP address: 133.133.1.2
```

+ *The bootp client has received a response and the IP address for this interface is 133.133.1.2.*

```
Phase 4 - Sending out Reverse DNS query onto Frame Relay
```

+ *rDNS is sending out a query looking for the hostname for IP address 133.133.1.2*

```
Phase 6 - getting hostname xsrnode-confg from tftp server into flash: startup-
config
```

+ *rDNS has responded with the hostname* **xsrnode** *which will be used in the TFTP transfer. RAI will try several file names if this file is not available from the server.*

```
Phase 7 - preparing node to execute startup-config
```

+ *TFTP transfer succeeded in copying the hostname file to the* **Flash: startup-config** *file.*

```
****************** REMOTE AUTO INSTALL TERMINATING*****************
```

+ *The RAI process is complete and is preoceding to system initialization where it will process the new* **`startup-config`** *file.*

Configuring RAI for DHCP over LAN

The following example configures DHCP server to be used with RAI over Ethernet. Note that there is no need for a DNS server because the **`startup-config`** name is provided by the DHCP server. Begin by creating an IP local pool which will include the Fast/GigabitEthernet interface address:

```
XSR(config)#ip local pool dhcp 200.1.0.0 255.255.255.01
```

Next, configure the interface that will service the remote device, set the IP address inside the pool defined earlier, and enable DHCP Server:

```
XSR(config)#interface GigabitEthernet 2
XSR(config-if<G2>)#ip address 200.1.0.4 255.255.255.0
XSR(config-if<G2>)#ip dhcp server
XSR(config-if<G2>)#no shutdown
```

Now configure the following DHCP Client parameters:

```
XSR(config)#ip dhcp pool dhcp
XSR(config-dhcp-pool)#lease 0 0 10
```

+ *This command sets a lease interval of 10 minutes*

```
XSR(config-dhcp-pool)#hardware-address 0001.f412.2334
```

+ *This command sets the MAC address of the client*

```
XSR(config-dhcp-pool)#host 200.1.0.66 255.255.255.0
```

+ *This command binds 200.1.0.66/24 to the earlier configured hardware address*

```
XSR(config-dhcp-pool)#option 12 instance 0 ascii etr1
```

+ *This command sets the Client hostname as* ***etr1***

```
XSR(config-dhcp-pool)#option 150 instance 0 ip 1.1.1.1
```

+ *This command configures the TFTP server IP address to 1.1.1.1*

```
XSR(config-dhcp-pool)#option 67 instance 0 ascii etr1-startup-confg
```

+ *This command enters the config-file name as startup-config*

Remember to save your configuration after all edits.

Configuring RAI over ADSL

In the following example, a remote XSR is connected to an ADSL network at the central site with a PPPoE server. A TFTP server runs on a separate machine - 192.168.72.118, while the PPPoE server runs on a CISCO router. The PPPoE server can reside on any other device providing PPPoE session termination and has a mechanism to direct TFTP broadcast packets to a specific IP address. A DNS server is not required with this method because RAI over ADSL uses the serial number of the XSR for the **`startup-config`** name.

The following is a CISCO configuration at the the central site:

```
vpdn enable
```

+ Enables a virtual private dial-up network configuration on the router.

```
vpdn-group 1
```

+ Creates a VPDN session group and links it to a virtual template.

```
accept-dialin
protocol pppoe
```

```
virtual-template 1
pppoe limit per-mac 10
```
+ This is an optional command.

```
pppoe limit max-sessions 32000
```
+ This is an optional command.

```
interface GigabitEthernet1/0/0
no ip address
negotiation auto
!
interface GigabitEthernet1/0/0.10
encapsulation dot1Q 20
pppoe enable
pppoe max-sessions 10
```
+ Optional. This command enables PPPoE and allows PPPoE sessions to be created through this sub-interface.

```
!
interface Virtual-Template1
ip unnumbered loop 0
mtu 1492
peer default ip address pool pool1
ppp authentication pap
ip helper-address 192.168.72.118
```
+ This is the address of the TFTP server.

```
ip directed-broadcast
```
+ This command configures the virtual template interface.

```
!
ip local pool pool1 192.168.0.1 192.168.0.100
username 0000019876543210 password 0 0000019876543210
```
+ Enter the remote XSR's serial number.

```
aaa new-model
!
aaa authentication ppp default local ! look at local database first
aaa authentication ppp dialins local
```
+ Specifies the IP local pool to use for address assignment.

When the RAI process begins, the remote XSR displays the following messages:

```
**************** PRESS ANY KEY TO TERMINATE REMOTE AUTO INSTALL ***************
Phase 2 - ADSL - searching for pvc's ...Training (60 sec)
```
+ The XSR begins training with the DSLAM, waiting 60 seconds.

```
Phase 2 - ADSL - searching for pvc's ...Training (54 sec)
Phase 2 - ADSL - searching for pvc's ...
```
+ Training is successful, discovery of VPI/VPCs begins.

```
Phase 2 - ADSL - searching for pvc's ...vpi/vci (0/0)
```
+ The XSR looks for PVC 0/0 and higher.

```
Phase 2 - ADSL - searching for pvc's ...vpi/vci (0/38)
```
+ The XSR looks for PVC 0/38 and higher.

```
Phase 3 - ADSL - trying to connect on 0/35 with snap PPPoE
```
+ PVC 0/35 is found, SNAP PPPoE encapsulation is applied and authentication tried if required.

```
Phase 3 - ADSL - waiting for IP to connect (54 sec)
```

+ The XSR waits one minute for the PPPoE connection to come up.

```
Phase 4 - ADSL - IP is connected on 0/35, prepare to load startup config
```

+ The XSR starts downloading the startup-file.

```
Phase 6 - ATM/ADSL - retrieving file 0000019876543210-confg from tftp server 25
5.255.255.255
```

+ The startup-config name is the serial number of the XSR.

```
Phase 7 - preparing node to execute startup-config
```

Configuring the XSR Name and User Information

1. At the CLI prompt, enter **enable** to acquire Privileged EXEC mode.
2. Enter **configure** to acquire Global mode.
3. Enter **hostname** <*your XSR designation*>.
4. Enter **username** <*name*> <**privilege** *level*> **password** <*cleartext | secret*> <*0 | 5*> <*password*>.
5. Enter **banner login** <*your welcome text*> to add a user login banner.

   Remember to save your configuration after all edits.

Setting User Name, Privilege and Password

The value <*name*> is the user's designation - for sake of clarity, often set as the name of the facility or site the XSR connects to. The value <*privilege level*> (0-15) prioritizes this user in terms of configuration rights with 15 as the highest and 0 the lowest (default). When you create a new user you can decide which privilege that user will have (if you are *admin*). For example, a user with privilege 7 will be allowed to execute only commands with privilege levels between 0 and 7.

Default privilege levels are defined for all commands and the *admin* user and are listed in the *XSR CLI Reference Guide* under the **`privilege`** command. You can change a command's default privilege by entering: **`privilege <configuration_mode> level <0-15> <command | command_group>`**.

The value <*cleartext | secret*> can be sent in the clear or encrypted with a **0** (the input password is not expected to be unencrypted so the XSR will encrypt it) or **5** (the input password is expected to already be encrypted so it will not be encrypted again). The value <*pass*> is the password associated with the specified name. The MD5 algorithm is encrypts the password.

Note: Newly created users are stored in the *startup config* file. You can also delete admin but only if you first create another level 15 user.

Setting the Clock

XSR 1800 and 3000 Series routers have an on-board Real Time Clock (RTC) chip with which to keep accurate time across the network. As an alternative to accessing a public time server, you can utilize the RTC as a time reference and propagate it by configuring XSRs as Simple Network Time Protocol (SNTP) servers or clients. XSR 1200 Series routers do not carry an RTC chip, however, and if your topology includes these devices you ***must*** synchronize them from an external source.

Enter the following command to configure the XSR as an SNTP client:

```
XSR(config)#sntp-client server [primary | A.B.C.D.][alternate | A.B.C.D.]
```

Enter the following command to configure the XSR as an SNTP server:

```
XSR(config)#sntp-server enable
```

Remember to save your configuration after all edits.

Configuring the LAN Ports

1. Enter **interface gigabitethernet** <*1* | *2* | *3*> to acquire Interface mode and select the first, second or third GigabitEthernet port.
2. Enter **ip address** <*xxx.xxx.xxx.xxx*> <*yyy.yyy.yyy.yyy*> where *x* is the IP address and *y* is the subnet mask of this GigabitEthernet port.
3. Enter **no shutdown** to keep the interface enabled.
4. Enter **show ip interface gigabitethernet** <*1* | *2* | *3*> to verify LAN settings.
5. Enter **copy running-config startup-config** to save your settings.

   Remember to save your configuration after all edits.

Configuring the WAN Ports

For ISDN PRI configuration, continue below; or see "BRI Configuration" on page 3-9, or "ADSL Configuration" on page 3-11.

PRI Configuration

1. Enter **controller** <*t1* | *e1*> <*slot* # | *card* # | *port* #> of the first installed T1/E1/ISDN-PRI NIM to acquire Controller mode and set up the physical port.
2. Enter **no shutdown** to keep the interface enabled.

   The above commands add either one channel-group *0* having 24 timeslots for the *T1* controller with default values for framing set to *ESF*, *B8ZS* line encoding, and *line* clock source, *or* one channel-group *0* having 31 timeslots for the *E1* controller including *crc4* framing, *hdb3* line encoding, and *line* clock source defaults. For a *non-default* configuration, go to Step 3.
3. Enter **clock source** <*line* | *internal* | *internal synchronization*> to select where the XSR will derive its timer for synchronized data transmission.

   The line source derives from the network, internal derives from a chip on the XSR, and internal synchronization derives from the first T1/E1/ISDN-PRI card by clock transfer.
4. Enter **no channel-group** <*number*> to delete the default group.
5. Enter **channel-group** <*number*> **timeslot** <*number*> <*speed*> <*number*> to create a channel group.

   This command allows multiple logical WAN interfaces to be created on a single channelized T1/E1/ISDN-PRI port, ranging from *0 - 23* for T1 lines, and *0 - 31* for E1 lines. Also, from *1 - 24* T1 and *1 - 31* E1 *timeslots* can be set. Channel speed options are 56 (T1) or 64 (E1) kbps.

   Note: Channel group and timeslot number ranges are *different*. Be sure to match them correctly and within the range. Also, when adding a *second* T1 or E1, be sure to begin channel numbering again at *0*.
6. Enter **framing** <*sf* | *esf* | *crc4* | *no-crc4*> to set the framing type.

The value you set must match the type and format offered by your service provider and must correlate with the NIM card you are configuring: *sf* or *esf* for T1 cards, and *crc4* or *no-crc4* for E1 cards.

7. Enter **linecode** <*ami* | *b8zs* | *hdb3*> to configure the encoding type.

   This setting must match your service provider's linecode type and type of NIM card installed: *B8ZS* for T1 only, *HDB3* for E1 only, and *AMI* for both T1/E1.

8. Enter **interface serial** <*slot #* | *card #* | *port #*> of the serial NIM card to acquire Interface mode and configure the logical interface.
9. Enter **encapsulation ppp** to set the encapsulation type.
10. Enter **ppp authentication** <*chap* [*ms-chap*] [*pap*] | *pap* [*ms-cha*p] [*chap*] | *ms-chap* [*chap*] [*pap*]> for the authentication type on the port.
11. Enter **ip address** <*xxx.xxx.xxx.xxx*> <*yyy.yyy.yyy.yyy*> where *x* is the IP address and *y* is the subnet mask of the serial port.
12. Enter **backup interface dialer** <*number*> to allow the serial interface to set the specified dialer interface as a dialed backup.
13. Enter **no shutdown** to keep the interface enabled.
14. Enter **show controller** <*T1* | *E1*> <*slot/card/port*> to verify NIM settings.
15. Enter **show interface serial** <*slot#* | *card#: channel#*> to verify serial port settings.
16. Enter **show ppp interface serial** <*card#*|*port#:channel#*> to display PPP status on the interface.
17. Enter **show dialer** to verify your dialer interface configuration.

    Remember to save your configuration after all edits.

BRI Configuration

ISDN BRI can be configured on a leased (over PPP or Frame Relay) or non-leased, switched line. Continue configuration with the BRI type of your choice.

BRI Leased Line

1. Enter interface **`bri 0:<1 | 2>`** to acquire Interface mode and select the BRI port and channel 1 or 2.
2. Enter **`leased-line <64 | 128>`** to acquired BRI interface mode and select 64 or 128 kbps line speed. Selecting 128 assigns B1 and B2 timeslots to channel 1 while 64 assigns either B1 or B2 timeslots to channel 1 or 2.
3. Enter **`ip address <xxx.xxx.xxx.xxx>/24`** to set an IP address for the BRI interface.
4. Enter **`encapsulation ppp`** to select PPP encoding.
5. Enter **`no shutdown`** to keep the BRI interface enabled.

BRI Leased Frame Relay

1. Enter **`interface bri 0:<1 | 2>.<1-30>`** to acquire BRI Interface mode and select the BRI port and channel 1 or 2.
2. Enter **`encapsulation frame-relay`** to select Frame Relay encoding.

3. Enter **no shutdown** to keep the BRI interface enabled.
4. Enter **frame-relay lmi-type <ilmi | ansi | q933a | auto | none>** to select the Local Management Interface type.
5. Enter interface **bri 0:<1 | 2>.<1-30> multi-point** to acquire BRI Sub-interface mode and select the BRI port, channel, and sub-interface.
6. Enter **ip address <xxx.xxx.xxx.xxx>/24** to set an IP address for the BRI interface.
7. Enter **frame-relay interface-dlci <16-1007>** to acquire Frame Relay DLCI Interface mode and assign a data-link connection identifier to the Frame Relay sub-interface.
8. Enter **no shutdown** to keep the BRI sub-interface enabled.

BRI Switched Line

1. Enter **interface bri 0** to acquire Interface mode and select the BRI port.
2. Enter **isdn switch-type <basic-5ess | basic-dms100 | basic-net3 | basic-ni1 | basic-ntt>** to select the Central Office switch type for the ISDN port.
3. Enter **isdn spid1 <SPID><LDR>** for the SPID (ISDN service) and LDR (local directory) telephone numbers.
4. Enter **isdn spid2 <SPID><LDR>** for a second SPID as needed.
5. Enter **no shutdown** to keep the BRI interface enabled.
6. Enter **dialer pool-member <1-255> priority <0-255>** to add a dialer pool and associated priority to this BRI interface. You can add additional dial pools as needed.
7. Enter **exit** to quit BRI Interface mode.
8. Enter **interface dialer <0-255>** to acquire Interface mode and select the Dialer port.
9. Enter **ip address <xxx.xxx.xxx.xxx/24** to set an IP address for the Dialer port.
10. Enter **encapsulation ppp** to select PPP encoding.
11. Enter **dialer string <phone number> class <Map Class name>** to specify the destination number and associated Map Class.
12. Enter any additional dialer strings as instructed above.
13. Enter **dialer pool <1-255>** to create a dial pool from which the dialer interface will select a physical interface.
14. Enter **show interface** to verify your ISDN and dialer configuration.
15. Enter **no shutdown** to keep the Dialer interface enabled.

Remember to save your configuration after all edits.

ADSL Configuration

ADSL can be configured using three different types of encapsulation: PPPoA, PPPoE, and IPoA. Continue configuration with the ADSL type of your choice.

PPPoE

The following commands configure a sample PPPoE topology. The first set configures the LAN interface with directed broadcasts prohibited.

```
XSR(config)#interface FastEthernet 1
XSR(config-if<F1>)#ip address 192.168.1.1 255.255.255.0
XSR(config-if<F1>)#no ip directed-broadcast
XSR(config-if<F1>)#no shutdown
```

The commands below configure the ATM interface and sub-interface with a negotiated IP address, PAP username and password, and ban keepalives. They also reset default PVC VPI and VCI values to those requested by the DSL provider. Notice that the Maximum Segment Size (MSS) is set to 1400 bytes for TCP SYN (synchronize) packets. Because a PC connected to a Fast/GigabitEthernet port may be unable to access Web sites if its MSS setting is too high, subtracting for the PPPoE, IP, TCP, and GRE headers (6, 20, 20, and 24 bytes, respectively) and the PPP Protocol ID should avoid that problem.

```
XSR(config)#interface ATM 0
XSR(config-if<ATM0/0>)#no shutdown
XSR(config-if<ATM0/0>)#interface ATM 0.1
XSR(config-if<ATM0/0.1>)#no shutdown
XSR(config-if<ATM0/0.1>)#encapsulation mux pppoe
XSR(config-if<ATM0/0.1>)#ip address negotiated
XSR(config-if<ATM0/0.1>)#ip mtu 1492
XSR(config-if<ATM0/0.1>)#ip tcp adjust-mss 1400
XSR(config-if<ATM0/0.1>)#ppp pap sent-username user@net password letmein
XSR(config-if<ATM0/0.1>)#no ppp keepalive
XSR(config-if<ATM0/0.1>)#pvc 0/100
```

The following optional commands configure two default routes:

```
XSR(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.10
XSR(config)#ip route 30.0.0.10 255.255.255.255 ATM 0.1
```

The following optional commands configure NAT:

```
XSR(config)#access-list 99 permit 192.168.1.0 0.0.0.255
XSR(config)#interface FastEthernet 1
XSR(config-if<F1>)#ip nat source list 99 assigned overload
```

PPPoA

Enter the following commands to configure PPPoA. The first set configures the LAN interface with directed broadcasts prohibited.

```
XSR(config)#interface FastEthernet 1
XSR(config-if<F1>)#ip address 192.168.1.1 255.255.255.0
XSR(config-if<F1>)#no ip directed-broadcast
XSR(config-if<F1>)#no shutdown
```

The commands below configure the ATM interface and sub-interface with a negotiated IP address, CHAP username and password, and bans keepalives.

```
XSR(config)#interface ATM 0
XSR(config-if<ATM0/0>)#no shutdown
XSR(config-if<ATM0/0.1>)#interface ATM 0.1
XSR(config-if<ATM0/0.1>)#no shutdown
XSR(config-if<ATM0/0.1>)#encapsulation snap pppoa
XSR(config-if<ATM0/0.1>)#ip address negotiated
XSR(config-if<ATM0/0.1>)#ip mtu 1492
XSR(config-if<ATM0/0.1>)#ip tcp adjust-mss 1400
XSR(config-if<ATM0/0.1>)#ppp chap hostname red password sox
XSR(config-if<ATM0/0.1>)#no ppp keepalive
```

Note: If you have configured a VPN tunnel and wish to avoid intermittent Web browser problems, add the **`crypto ipsec df-bit clear`** command to your configuration.

IPoA

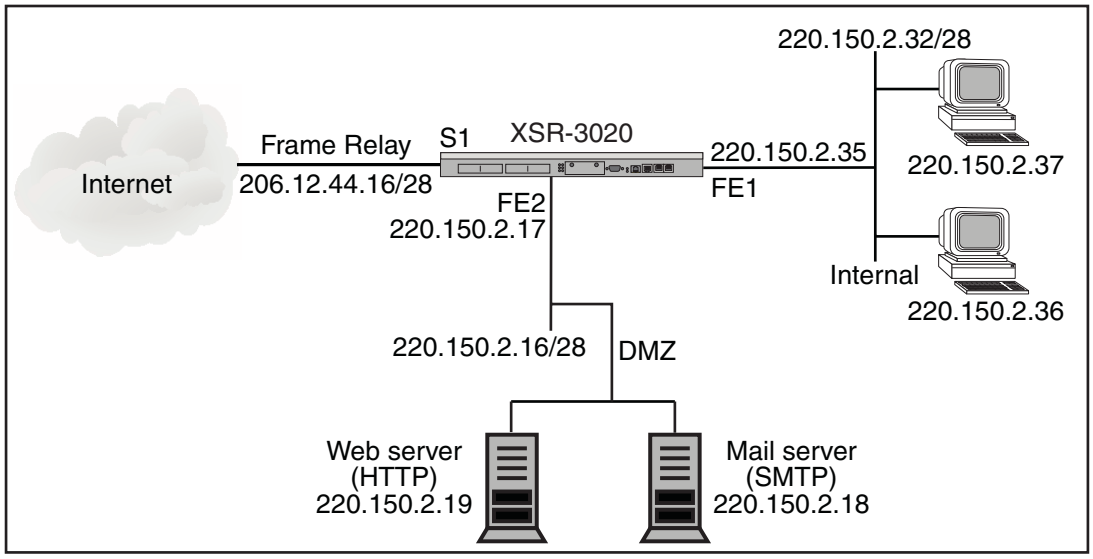
Enter the following commands to configure a IPoA topology:

```
XSR(config)#interface ATM 0
XSR(config-if<ATM0/0>)#no shutdown
XSR(config-if<ATM0/0>)#interface ATM 0.1
XSR(config-if<ATM0/0.1>)#encapsulation snap ipoa
XSR(config-if<ATM0/0.1>)#ip address 192.168.1.1 255.255.255.0
XSR(config-if<ATM0/0.1>)#ip mtu 1492
XSR(config-if<ATM0/0.1>)#exit
XSR(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.10
XSR(config)#ip route 30.0.0.10 255.255.255.255 ATM 0.1
```

Firewall Sample Configuration

In this scenario, the XSR acts as a router connecting a branch office to the Internet, as illustrated in Figure 3-1. The branch office has two servers (Web and Mail) accessible from the external world and an internal network of hosts which are protected from the external world by the firewall. The Web and Mail servers are part of the DMZ and considered internal by the XSR. Note that some commands have been abbreviated.

Figure 3-1 XSR with Firewall Topology



In this configuration, the firewall provides protected access from the *private* to *dmz* networks. That is, access is restricted to Web and mail traffic only. The hosts in the *private* network are provided full access to the Internet but access is *denied* from the Internet to the private *network*. Also, all Java and ActiveX pages, IP options, IP broadcast and multicast packets are banned.

Begin by specifying network objects for *private, dmz*, and *Mgmt* networks:

```
XSR(config)#ip firewall network dmz 220.150.2.16 mask 255.255.255.240 internal
XSR(config)#ip firewall network private 220.150.2.32 mask 255.255.255.240
internal
XSR(config)#ip firewall network Mgmt 220.150.2.35 mask 255.255.255.0 internal
```

Log only critical events:

```
XSR(config)#ip firewall logging event-threshold 3
```

Set policies between the *dmz* and *external* networks. Note that policy objects and names are *case-sensitive* and you must cite network names *exactly*:

```
XSR(config)#ip firewall policy a1 private dmz HTTP allow
XSR(config)#ip firewall policy a2 dmz private HTTP allow
XSR(config)#ip firewall policy a3 private dmz HTTP allow
XSR(config)#ip firewall policy a4 dmz private HTTP allow
```

Set the policies between the *dmz* and *external* networks:

```
XSR(config)#ip firewall policy a5 ANY_EXTERNAL dmz SMTP allow
XSR(config)#ip firewall policy a6 dmz ANY_EXTERNAL SMTP allow
XSR(config)#ip firewall policy a7 ANY_EXTERNAL dmz SMTP allow
XSR(config)#ip firewall policy a8 dmz ANY_EXTERNAL SMTP allow
```

Set policies to allow any traffic from *private* to *external* and *Mgmt* networks:

```
XSR(config)#ip firewall policy a9 private ANY_EXTERNAL ANY_TCP allow
XSR(config)#ip firewall policy Telnetsess Mgmt Mgmt Telnet allow bidirectional
```

Allow ICMP traffic to pass from the *dmz* to *private*, *private* to *all external, and all external* to *private* networks:

```
XSR(config)#ip firewall filter allowICMP private dmz protocol-id 1
XSR(config)#ip firewall filter allowICMP private ANY_EXTERNAL protocol-id 1
XSR(config)#ip firewall filter allowICMP ANY_EXTERNAL dmz protocol-id 1
```

Trial load the completed configuration into the firewall engine, and if successful, load the configuration:

```
XSR(config)#ip firewall load trial
XSR(config)#ip firewall load
```

Complete LAN and WAN interface configuration:

```
XSR(config)#interface gigabitethernet 1
XSR(config-if<G1>)#ip address 220.150.2.35 255.255.255.0
XSR(config-if<G1>)#no shutdown

XSR(config)#interface gigabitethernet 2
XSR(config-if<G2>)#ip address 220.150.2.17 255.255.255.0
XSR(config-if<G2>)#no shutdown

XSR(config)#interface serial 1/0:0
XSR(config-if<S1/0:0>)#ip address 206.12.44.16 255.255.255.0
XSR(config-if<S1/0:0>)#no shutdown
```

Globally enable the firewall. Even though you have configured and loaded the firewall, only invoking the following command "turns on" the firewall. Once enabled, if you are remotely connected, the firewall will close your session. Simply login again.

```
XSR(config)#ip firewall enable
```

For more Firewall configuration examples, refer to the *XSR User's Guide*.

Setting Up RIP Routing

The following commands configure a GigabitEthernet and Serial interface to support RIP with additional functionality as an option:

1. Enter **interface gigabitethernet** <*1* | *2* | *3*> to acquire Interface mode and select the first, second, or third GigabitEthernet port.
2. Enter **ip address** <*xxx.xxx.xxx.xxx*> <*yyy.yyy.yyy.yyy*> where *x* is the IP address and *y* is the subnet mask of this GigabitEthernet port.
3. Enter **no shutdown** to keep the interface enabled.
4. Enter **interface serial** <*slot #* | *card #* | *port #*> of the serial NIM card to re-acquire Interface mode and select slot, card and port numbers.
5. Enter **ip address** <*xxx.xxx.xxx.xxx*> <*yyy.yyy.yyy.yyy*> where *x* is the IP address and *y* is the subnet mask of the serial port.
6. Enter **ip rip authentication mode text** if you want to set clear-text authentication. If you enter this command, continue with the Step 7, otherwise, go to Step 8.
7. Enter **ip rip authentication key-string** <*text*> to specify a text string for authentication.
8. Enter **no shutdown** to keep the interface enabled.
9. Enter **ip rip send version** <*1* | *2*> to allow the RIP version of update transmissions. Version 1 is the default value.
10. Enter **ip rip receive version** <*1* | *2*> to allow a RIP version of updated transmissions. Accept both RIP V1 and V2 is the default value.
11. Enter **router rip** to acquire Router configuration mode and enable RIP routing.

12. Enter **network** <*xxx.xxx.xxx.xxx*> *(IP address)* of the network to be advertised. Repeat the command to configure additional networks.
13. Enter **passive-interface** *type num* if you want to prevent RIP transmissions on the interface.
14. Enter **no receive-interface** if you want to disable reception of RIP updates on the interface.

    Remember to save your configuration after all edits.

For more RIP configuration examples, refer to the *XSR User's Manual*.

Configure OSPF Routing

The following OSPF configuration adds two networks to OSPF areas and sets the cost of sending traffic on the serial interface:

1. Enter **interface gigabitethernet** <*1* | *2* | *3*> to acquire Interface mode and select the first, second, or third GigabitEthernet port.
2. Enter **ip address** <*xxx.xxx.xxx.xxx*> <*yyy.yyy.yyy.yyy*> where *x* is the IP address and *y* is the subnet mask of this GigabitEthernet port.
3. Enter **no shutdown** to keep the interface enabled.
4. Enter **interface serial** <*slot #* | *card #* | *port #*> of the serial NIM card to re-acquire Interface mode and select slot, card and port numbers.
5. Enter **ip address** <xxx.xxx.xxx.xxx> <yyy.yyy.yyy.yyy> where *x* is the IP address and *y* is the subnet mask of the serial port.
6. Enter **no shutdown** to keep the interface enabled.
7. Enter **encapsulation ppp** to set the correct encapsulation type.
8. Enter **ip ospf cost** <*1-65535*> to set the cost of receiving a packet on this interface.
9. Enter **router ospf** to acquire Router configuration mode and enable OSPF routing.
10. Enter **network** <xxx.xxx.xxx.xxx> **area** <*area-id*> of the network to be advertised. Repeat the command to configure additional networks.

    Remember to save your configuration after all edits. For more OSPF configuration examples, refer to the *XSR User's Manual*.

Configuring Frame Relay Point to Point Networks

The following Frame Relay configuration sets up point-to-point networks on *Central* and *Branch* XSRs. On the *Central* XSR, perform these steps:

1. Enter **interface serial** <*slot #* | *card #* | *port #*> of the serial NIM card to acquire Interface mode and select a slot, card and port number.
2. Enter **encapsulation frame-relay** to set the encapsulation type.
3. Enter **no shutdown** to keep the interface enabled.
4. Enter **frame-relay lmi-type** <*ilmi* | *ansi* | *q933a* | *auto* | *none*> to manually select the Link Management Interface protocol type to use on the port or retain the default type *auto*.
5. Enter **media-type V35** to match the correct cabling interface. The default media type for Frame Relay is RS-232.
6. Enter **frame-relay traffic-shaping** to enable congestion control.

7. Enter **map-class frame-relay** <*name*> to designate this map-class and acquire Map-Class mode.
8. Enter **frame-relay cir out** <*bits*> to set the outgoing CIR (the default is 56000 bps). Refer to the *XSR User's Guide* for more details.
9. Enter **frame-relay bc out** <*bits*> to set the Burst size for this map-class. Refer to the *XSR User's Manual* for further directions.
10. Enter **frame-relay be out** <*rate*> to set the excess Burst site for this map-class. Refer to the *XSR User's Manual* for more directions.
11. Enter **interface serial** <*slot #* | *card #* | *port #* | *subinterface#*> <*point*> of the serial NIM card to acquire Sub-interface mode, select the point-to-point connection type and begin configuring this sub-interface.
12. Enter **no shutdown** to enable the sub-interface.
13. Enter **ip address** <*xxx.xxx.xxx.xxx*> <*yyy.yyy.yyy.yyy*> where *x* is the IP address and *y* is the subnet mask of this sub-interface.
14. Enter **frame-relay interface-dlci** <*16 - 1007*> to assign a Data-link Connection Identifier (DLCI) to this sub-interface. DLCIs are provisioned by your service provider.
15. Enter **class** <*name*> to designate the map-class which will be assigned to the earlier specified DLCI. The class name often refers to the speed of the connection such as *SlowLink* for a 64000 bps link.
16. Repeat the previous steps on the *Branch* XSR.

    Remember to save your configuration after all edits. Refer to the *XSR User's Guide* for more information.

Setting Up an SNMP Community String, Traps and V3 Values

1. Enter **snmp-server community** <*string*> <*ro* | *rw*> <ACL #> to create an SNMP community with an optional ACL on the XSR. Although SNMP is disabled by default, entering any SNMP configuration command except **snmp-server disable** will enable the SNMP server.

   You can choose either Read Only or Read/Write privileges and can create read-only or read-write community strings. Also, community-based write access is available for the *ct-download* MIB only. For write access to other MIBs, use SNMPv3. Also, a RW community is *unnecessary* for SNMPv3.

Note: Only standard ACLs can be applied to SNMP configuration commands.

2. Enter **snmp-server host** <*IP address*> **traps** <*community-string* [*snmp*]> to specify where traps are sent.
3. Enter **snmp-server location** <*location-string*> to specify where the SNMP device is sited.
4. Enter **snmp-server enable traps** *snmp authentication* to define which traps are sent.
5. *Optional* . For SNMPv3, enter **`snmp-server group <name> v3`** {*auth* | *nonauth* | *priv*} read <name> **`write`** <*name*> to add a group.

Groups offer users authorization choices and read/write privileges.

Note: Because only one operator can set the XSR at any time, you must exit Global mode to perform SNMPv3 configuration. Otherwise, the SNMP set request will fail with the "resource unavailable" message. This rule applies to configuration values, not image downloads.

6. *Optional*. For SNMPv3, enter **`snmp-server view`** <*name*> {*oid-tree* | *treeEntryName*}{*included* | *excluded*} to specify a view.

   Views offer users selective access to the family tree or Object IDs.

7. *Optional*. For SNMPv3, enter **`snmp-server user`** <*username*> <*group name*> **`v3`** [*encrypted*][*auth* {*md5* | *sha*} **`auth-password`** [*priv des56 priv-password*]]} to add a user.

   Users can have different levels of encryption and passwords. Remember to save your configuration after all edits. Refer to the *User's Guide* and *CLI Reference Guide* for more information.

Note: To restart the XSR using NetSight or SNMP management programs, you must enter the **snmp-server system-shutdown** command.

Configuring Message Logging and Severity Level

1. Enter **logging** <*console* | *buffer* | *monitor* | *snmp* | *A.B.C.D* | *file*> <*high* | *medium* | *low* | *debug*> to direct where error messages are sent and what degree of severity they will reflect.

   Messages stored to *buffer* are saved to the XSR's RAM, those stored to *monitor* are displayed on active Telnet CLI sessions, those stored to A.B.C.D. are saved in the IP address of the associated SYSLOG server. Refer to the *XSR CLI Reference* and *User Guide* for more information about severity levels.

   Typically, only HIGH severity alarms are logged to red flag critical events and those requiring operator intervention. Also, the DEBUG alarm level is meant for maintenance personnel only.

   The XSR may discard LOW and DEBUG level alarms if the system is too occupied to deliver them. The number of discarded messages is displayed by the following line in **`show logging`** command output:

   ```
   Discards: high=0 medium=0 low=4 debug=22
   ```

2. Enter **show logging** to verify the logging configuration.

   When the XSR has been up and running for a while more data will be shown in this display. For a detailed list of most alarms and events generated by the router, refer to the *XSR User Guide*. Remember to save your configuration after all edits.

Viewing Your Configuration

1. Enter **show running-config** to verify your current configuration.

   The XSR will display the commands you issued up to this point. Default values are not displayed.

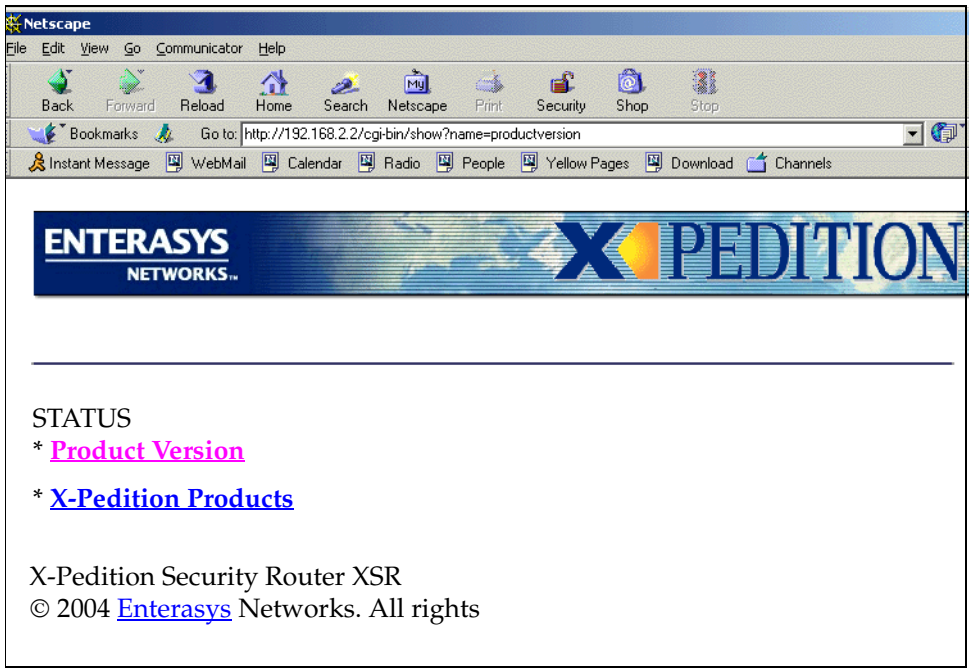
Note: All **show** commands can be entered in privileged EXEC mode - **XSR#** - or Global configuration mode - **XSR(config)#**.

Connecting Remotely via the Web

1. Enter **configure** to acquire Configuration mode.
2. Enter **ip http server enable** to access the XSR over the Web.
3. Point your terminal's Web browser at the XSR's IP address. Enter **http://<XSR IP address>**.

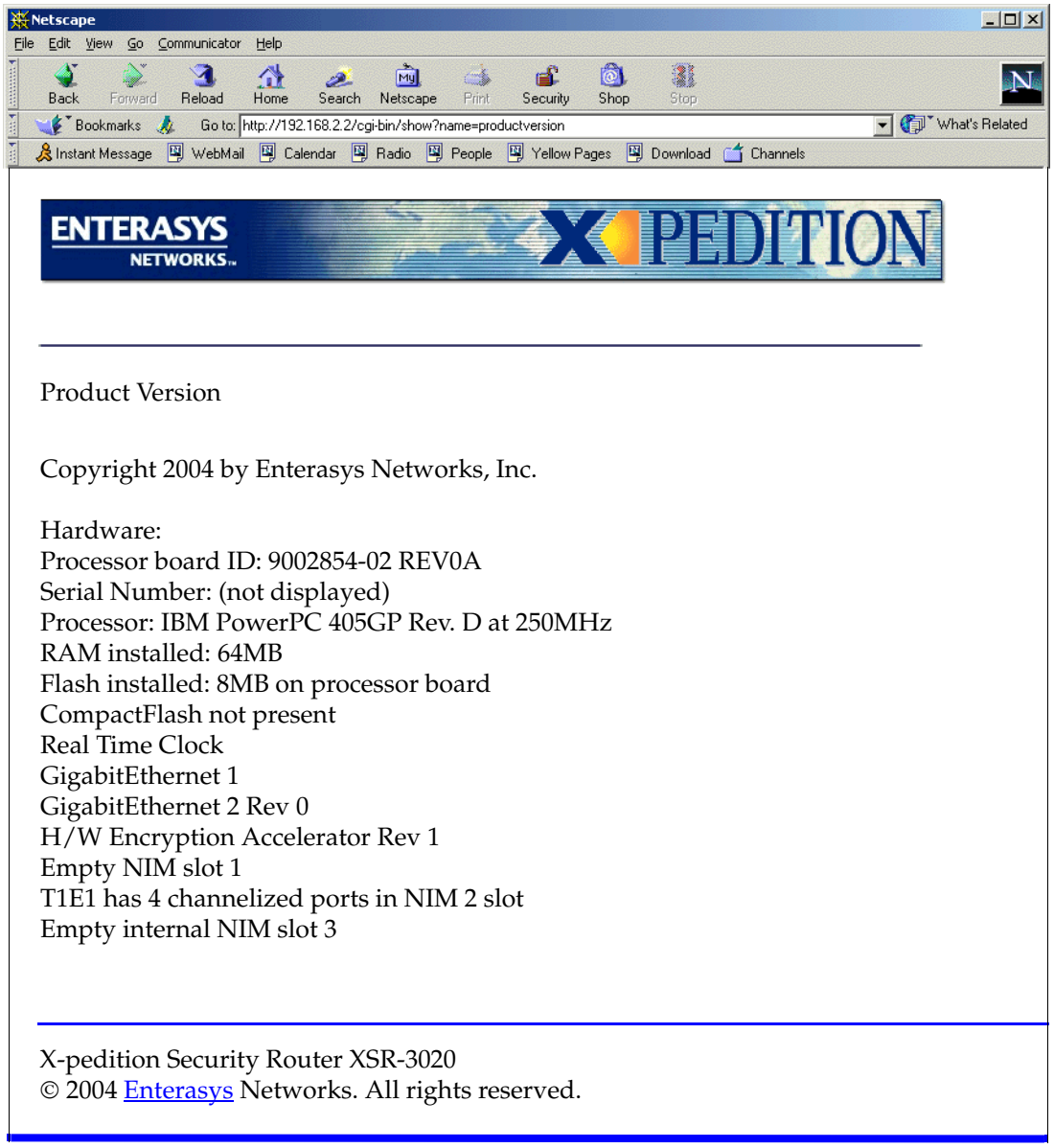
   The initial Web access window appears as shown in Figure 3-2.

Figure 3-2 Initial Web Access Window



Click on Product Version to bring up the Product Version window for a host of hardware, bootrom, and software information as shown in Figure 3-3.

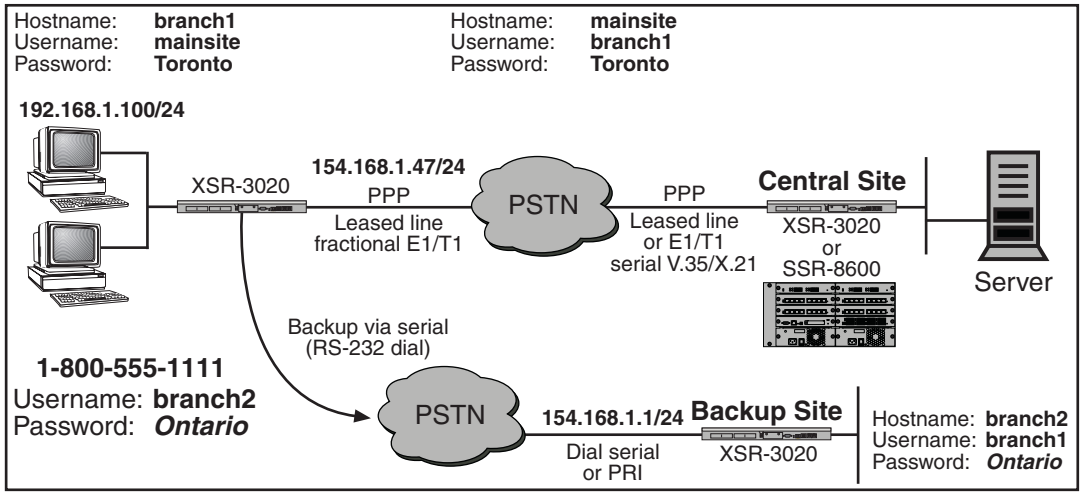
Figure 3-3 Web Product Version Window



LAN-PPP Services Sample Configuration

The sample configuration below, see Figure 3-4, creates a PPP, fractional T1 leased line connection from the XSR branch node to the Central Site router and a backup serial dialup link to the Backup Site regional router.

Figure 3-4 Sample LAN-PPP Services Configuration



The following script configures the LAN-PPP services topology shown above.

```
XSR>enable
```
+ *Acquires Privileged EXEC mode*

```
XSR#configure
```
+ *Acquires Global configuration mode*

```
XSR(config)#hostname branch1
```
+ *Configures the local hostname*

```
XSR(config)#username mainsite password secret 0 Toronto
```
+ *Configures first username and password for CHAP*

```
XSR(config)#username branch2 password secret 0 Ontario
```
+ *Configures second username and encrypted password for CHAP*

```
XSR(config)#interface gigabitethernet 1
```
+ *Configures local LAN interface and acquires Interface mode*

```
XSR(config-if<G1>)#ip address 192.168.1.100 255.255.255.0
```
+ *Enables IP address for GigabitEthernet interface*

```
XSR(config-if<G1>)#no shutdown
```
+ *Enables the interface*

```
XSR(config)#controller t1 0/1/0
```
+ *Sets up main link connection: T1 NIM in slot 1, port 0 and acquires Controller mode*

```
XSR(config-controller<T1-1/0>)#clock source line
```
+ *Sets external clocking of T1 NIM*

```
XSR(config-controller<T1-1/0>)#no channel-group 0
```
+ *Deletes default channel setup*

```
XSR(config-controller<T1-1/0>)#channel 0 timeslot 1-4,7,9-15
```
+ *Adds channel group 0 mapping to time slots 1-4, 7, and 9-15*

```
XSR(config-controller<T1-1/0>)#framing esf
```
+ *Begins configuring T1 channel values: sets T1 line frame type*

```
XSR(config-controller<T1-1/0>)#linecode b8zs
```
+ *Sets T1 encoding*

```
XSR(config-controller<T1-1/0>)#no shutdown
```
+ *Enables T1 controller*

```
XSR(config)#interface serial 1/0:0
```
+ *Configures Serial interface 1, port 1 using channel group 0 and acquires Interface mode*

```
XSR(config-if<S1/0:0>)#encapsulation ppp
```
+ *Enables PPP encapsulation*

```
XSR(config-if<S1/0:0>)#ppp authentication chap
```
+ *Configures CHAP authentication on the interface*

```
XSR(config-if<S1/0:0>)#ip address 154.68.1.47 255.255.255.0
```
+ *Enables IP address for serial interface 1/0*

```
XSR(config-if<S1/0:0>)#backup interface dialer 5
```
+ *Sets dialed interface as a dialed backup*

```
XSR(config-if<S1/0:0>)#no shutdown
```
+ *Enables the interface*

```
XSR(config)#router rip
```
+ *Enables RIP routing and goes to Router mode*

```
XSR(config-router)#network 192.168.1.100
```
+ *Configures a network RIP will advertise its routes to*

```
XSR(config-router)#network 154.68.1.0
```
+ *Configures a second network RIP will advertise its routes to*

```
XSR(config-router)#network 164.55.7.0
```
+ *Configures a third network RIP will advertise its routes to*

```
XSR(config)#interface dialer 5
```
+ *Adds backup interface and acquires Interface mode*

```
XSR(config-if<D5>)#dialer pool 3
```
+ *Adds a dialer pool on interface*

```
XSR(config-if<D5>)#dialer string 18005555555
```
+ *Sets backup phone #*

```
XSR(config-if<D5>)#encapsulation ppp
```
+ *Enables PPP encapsulation on port*

```
XSR(config-if<D5>)#ppp authentication chap
```
+ *Sets CHAP on port*

```
XSR(config-if<D5>)#ip address 164.55.7.22 255.255.255.0
```
+ *Enables the IP address for dialer interface 5*

```
XSR(config-if<D5>)#no shutdown
```
+ *Enables the interface*

```
XSR(config)#interface serial 2/0
```
+ *Configures backup interface: Serial card in slot 2, port 0 and acquires Interface mode*

```
XSR(config-if<S2/0>)#dialer pool-member 3
```
+ *Adds a dial pool*

```
XSR(config-if<S2/0>)#physical-layer sync
```
+ *Sets synchronous mode*

```
XSR(config-if<S2/0>)#no shutdown
```
+ *Enables the interface*

Frame Relay WAN Link with PPP Backup Sample Configuration

The sample configuration below, similar to the preceding configuration except that the cloud supporting the primary line is Frame Relay rather than Public Service Telephone Network, configures one LAN port, the Frame Relay WAN, QoS, OSPF routing, DHCP Relay, IP broadcast forwarding, SNMP with ACL rules, and access lists.

Configure Users and Passwords

```
XSR(config)#username bob password cleartext bobspassword
```
+ *Adds a user and unencrypted password*

Configure LAN Interface

```
XSR(config)#interface gigabitethernet 1
```
+ *Configures the local LAN port and acquires Interface mode*

```
XSR(config-if<G1>)#ip address 192.168.1.100 255.255.255.0
```
+ *Enables the IP address for the GigabitEthernet port*

```
XSR(config-if<G1>)#no shutdown
```
+ *Enables the interface*

Configure Quality of Service

```
XSR(config)#access-list 129 permit udp 192.168.1.0 0.0.0.255 any eq 554
```
+*Adds a UDP filter matching the source network and any destination address to port 554*

```
XSR(config)#access-list 129 permit tcp 192.168.1.0 0.0.0.255 any eq 554
```
+*Adds a TCP filter matching the source network and any destination address to port 554*

```
XSR(config)#access-list 130 permit ip any host 192.168.2.75
```
+ *Adds an IP filter matching any source address to the specified destination address*

```
XSR(config)#access-list 131 permit tcp any any eq 20
```
+ *Adds a TCP filter which matches any source address and destination address to port 20*

```
XSR(config)#access-list 132 permit tcp any any eq 21
```
+ *Adds a TCP filter which matches any source and destination address to port 21*

```
XSR(config)#access-list 133 permit tcp any any eq 80
```
+ *Adds a TCP filter which matches any source and destination address to port 80*

```
XSR(config)#class-map rtp-class
```
+ *Adds a class-map and acquires Class Map mode*

```
XSR(config-cmap<rtp-class>)#match access-group 129
```
+ *Assigns ACL 129 to this class map*

```
XSR(config)#class-map priority-server
```
+ *Adds a class-map and acquires Class Map mode*

```
XSR(config-cmap<priority-server>)#match access-group 130
```
+ *Assigns ACL 130 to this class map*

```
XSR(config)#class-map match-any data_class
```
+ *Adds a class-map and acquires Class Map mode*

```
XSR(config-cmap<data_class>)#match access-group 131
```
+ *Assigns ACL 131 to this class map*

```
XSR(config-cmap<data_class>)#match access-group 132
```
+ *Assigns ACL 132 to this class map*

```
XSR(config-cmap<data_class>)#match access-group 133
```
+ *Assigns ACL 133 to this class map*

```
XSR(config)#policy-map priority-policy
```
+ *Adds a policy map and acquires Policy Map mode*

```
XSR(config-pmap<priority-policy>)#class rtp_class
```
+ *Adds a queue for this policy map and acquires Class sub-mode*

```
XSR(config-pmap-c<priority-policy>)#priority high 30 3200
```
+ *Gives high priority queue a peak 30% of bandwidth and a burst size of 3200 bits per second*

```
XSR(config-pmap-c<priority-policy>)#set ip dscp ef
```
+ *Configures IP precedence to match packets with Expedited Forwarding*

```
XSR(config-pmap<priority-policy>)#class priority-server
```
+ *Adds another queue for this policy map and enters Class sub-mode*

```
XSR(config-pmap-c<priority-server>)#priority medium 20 6400
```
+ *Gives medium priority queue a peak 20% of bandwidth & burst size of 6400 bits per second*

```
XSR(config)#policy-map data_policy
```
+ *Adds a policy map and acquires Policy Map mode*

```
XSR(config-pmap<data_policy>)#class data_class
```
+ *Adds a queue for this policy map and acquires Class sub-mode*

```
XSR(config-pmap-c<data_class>)#police 24000 2400 4800 conform-action transmit
exceed-action set-dscp-transmit 23 violate-action drop
```
+ *Sets traffic policing at an average rate of 24000 bits per second, a normal burst size of 2400 bits per second, and an excess burst size of 4800 bits per second. Packets conforming to values are sent, those exceeding are set to a DSCP value of 23 and those violating values are dropped.*

```
XSR(config-pmap-c<data_class>)#bandwidth percent 50
```
+ *Gives the class a minimum 50% of the bandwidth*

Configure WAN/Frame Relay Port

This port's IP address is 154.68.1.47. The attached switch operates at 128,000 bps, with *auto* LMI type, and traffic shaping enabled. Any QoS values set will be applied to the DLCIs: do not apply QoS to the port, it is not recommended on Frame Relay connections. Note that some commands are abbreviated.

```
XSR(config)#interface serial 1/0
```
+ *Configures Frame Relay interface: Serial card in slot 1, port 0 and acquires Interface mode*

```
XSR(config-if<S1/0>)#media-type v35
```
+ *Selects type for Frame Relay*

```
XSR(config-if<S1/0>)#no shutdown
```
+ *Enables the interface*

```
XSR(config-if<S1/0>)#encapsulation frame-relay
```
+ *Enables FR encapsulation*

```
XSR(config-if<S1/0>)#frame-relay class CLASS-FRP
```
+ *Adds a FR map class*

```
XSR(config-if<S1/0>)#frame-relay traffic-shaping
```
+ *Enables map class values*

```
XSR(config)#interface serial 1/0.1 multipoint
```
+ *Adds FR port: serial card in slot 1, port 0, sub-interface 1 for multipoint connections and acquires Interface mode*

```
XSR(config-if<S1/0.1>)#frame-relay interface-dlci 33
```
+ *Adds PVC #33*

```
XSR(config-if<S1/0.1-33>)#no shutdown
```
+ *Enables the DLCI port*

```
XSR(config-if<S1/0.1-33>)#ip address 154.68.1.47 255.255.255.0
```
+ *Configures the IP address of the port*

```
XSR(config)#interface serial 1/0.2 multipoint
```
+ *Configures FR port: Serial card in slot 1, port 0, sub-interface 2 for multipoint links and acquires Interface mode*

```
XSR(config-if<S1/0.2>)#frame-relay class CLASS_SI
```
+ *Adds another FR map class*

```
XSR(config-if<S1/0.2>)#frame-relay interface-dlci 16
```
+ *Adds PVC #16 and acquires DLCI 16 sub-mode*

```
XSR(config-if<S1/0.2-16>)#class CLASS_DLCI
```
+ *Assigns the specified map class to DLCI 16*

```
XSR(config-if<S1/0.2-16>)#ip address 154.68.2.1 255.255.255.0
```
+ *Configures the IP address of DLCI 16*

```
XSR(config-if<S1/0.2-16>)#no shutdown
```
+ *Enables DLCI 16 interface*

Apply QoS

```
XSR(config)#map-class frame-relay CLASS-FRP
```
+ *Adds a FR map class and acquires FR Map Class mode*

```
XSR(config-map-class<CLASS-FRP>)#frame-relay cir out 48000
```
+ *Sets this map class' CIR rate at 48000 bits per second*

```
XSR(config-map-class<CLASS-FRP>)#frame-relay bc out 4000
```
+ *Sets this map class' committed burst size to 4000 bits*

```
XSR(config-map-class<CLASS-FRP>)#frame-relay be out 3000
```
+ *Sets this map class' excess burst size to 3000 bits*

```
XSR(config-map-class<CLASS-FRP>)#frame-relay adaptive-shaping
```
+ *Enables BECN (traffic shaping) for this map class*

```
XSR(config-map-class<CLASS-FRP>)#service-policy output data_policy
```
+ *Attaches this policy to the map class*

```
XSR(config)#map-class frame-relay CLASS-SI
```
+ *Adds another FR map class and acquires Frame Relay Map Class mode*

```
XSR(config-map-class<CLASS-SI>)#frame-relay cir out 30000
```
+ *Sets this map class' CIR rate at 30,000 bits per second*

```
XSR(config-map-class<CLASS-SI>)#frame-relay bc out 5000
```
+ *Sets this map class' committed burst size to 5000 bits*

```
XSR(config-map-class<CLASS-SI>)#frame-relay be out 3000
```
+ *Sets this map class' excess burst size to 3000 bits*

```
XSR(config-map-class<CLASS-SI>)#frame-relay adaptive-shaping
```
+ *Enables BECN (traffic shaping) for this map class*

```
Router(config-map-class<CLASS-SI>)#service-policy HighOutput
```
+ *Attaches this policy to the map class*

```
XSR(config)#map-class frame-relay CLASS-DLCI
```
+ *Adds another Frame Relay map class and acquires Frame Relay Map Class mode*

```
XSR(config-map-class<CLASS-DLCI>)#frame-relay cir out 50000
```
+ *Sets this map class' CIR rate at 50,000 bits per second*

```
XSR(config-map-class<CLASS-DLCI>)#frame-relay bc out 4000
```
+ *Sets this map class' committed burst size to 4000 bits*

```
XSR(config-map-class<CLASS-DLCI>)#frame-relay be out 1000
```
+ *Sets this map class' excess burst size to 1000 bits*

```
XSR(config-map-class<CLASS-DLCI>)#frame-relay adaptive-shaping
```
+ *Enables BECN (traffic shaping) for this map class*

```
XSR(config-map-class<CLASS-DLCI>)#service-policy output priority-policy
```
+ *Attaches this policy to the map class*

Configure OSPF Routing

```
XSR(config)#router ospf 1
```
+ *Enables OSPF with a router ID and acquires Router mode*

```
XSR(config-router)#network 192.168.1.0 0.0.0.255 area 0.0.0.10
```
+ *Configures the area ID for the specified network*

```
XSR(config-router)#network 154.68.1.0 0.0.0.255 area 0.0.0.0
```
+ *Configures another area ID for the specified network*

Configure More Access Lists

The following ACLs deny any packets to or from network 192.168.1.15 as they enter or leave FastEthernet 1 interface, and permit traffic to or from subnet 192.168.2.*xx* while denying any other traffic.

```
XSR(config)#access-list 125 deny ip any host 192.168.1.15
```

```
XSR(config)#access-list 125 deny ip host 192.168.1.15 any
XSR(config)#access-list 125 permit ip 192.162.2.0 0.0.0.255 any
XSR(config)#access-list 125 permit ip 192.162.2.0 0.0.0.255
XSR(config)#interface fastethernet 1
XSR(config-if<F1>)#ip access-group 125 in
XSR(config-if<F1>)#ip access-group 125 out
```

Configure DHCP/BOOTP Relay

```
XSR(config)#interface gigabitethernet 1
```
+ *Adds GigabitEthernet port 1 and acquires Interface mode*

```
XSR(config-if<G1>#ip helper-address 192.168.1.120
```
+ *Marks destination IP address for UDP broadcasts*

Configure the Dial Backup Connection

```
XSR(config)#interface serial 1/0
```
+ *Adds serial port 1 and acquires Interface mode*

```
XSR(config-if<S1/0>)#encapsulation ppp
```
+ *Enables PPP encapsulation*

```
XSR(config-if<S1/0>)#ip address 192.31.27.80 255.255.255.0
```
+ *Sets the IP address on the interface*

```
XSR(config-if<S1/0>)#backup interface dialer 1
```
+ *Adds a backup dialer interface*

```
XSR(config-if<S1/0>)#backup delay 2 2
```
+ *Sets the interval that elapses after the primary interfaces fails and comes up*

```
XSR(config-if<S1/0>)#no shutdown
```
+ *Enables the interface*

```
XSR(config)#interface serial 2/0
```
+ *Adds serial port 2 and acquires Interface mode*

```
XSR(config-if<S2/0>)#dialer pool-member 1
```
+ *Adds a dial pool member*

```
XSR(config-if<S2/0>)#physical-layer sync
```
+ *Sets synchronous mode*

```
XSR(config-if<S2/0>)#no shutdown
```
+ *Enables the interface*

```
XSR(config)#int dialer 1
```
+ *Adds dialer interface and acquires Dialer Interface mode*

```
XSR(config-if<D1>)#encapsulation ppp
```
+ *Enables PPP encapsulation*

```
XSR(config-if<D1>)#ip address 192.31.27.84 255.255.255.0
```
+ *Sets the IP address on the interface*

```
XSR(config-if<D1>)#dialer string 4165557922
```
+ *Sets dialer phone #*

```
XSR(config-if<D1>)#dialer wait-for-carrier 30
```
+ *Specifies the period the XSR will wait for a connection from the service provider*

```
XSR(config-if<D1>)#di pool 1
```
+ *Specifies the dial pool from which calls originate*

```
XSR(config-if<D1>)#no shutdown
```
+ *Enables the dial interface*

Configure SNMP

The previously configured ACL will be applied to all SNMP requests. Stricter ACLs can be written if tighter security controls are required.

```
XSR(config)#snmp-server community toMonitor1 ro 26
```
+ *Adds an SNMP community with read-only privileges attached to ACL 26*

```
XSR(config)#snmp-server community toConfigure1 rw 26
```
+ *Adds another SNMP community with read-write privileges attached to ACL 26*

```
XSR(config)#snmp-server enable traps
```
+ *Enables traps to be transmitted*

```
XSR(config)#snmp-server contact support@enterasys.com
```
+ *Specifies contact information for the management server*

```
XSR(config)#snmp location "HQ 2nd floor"
```
+ *Specifies the server locationr*

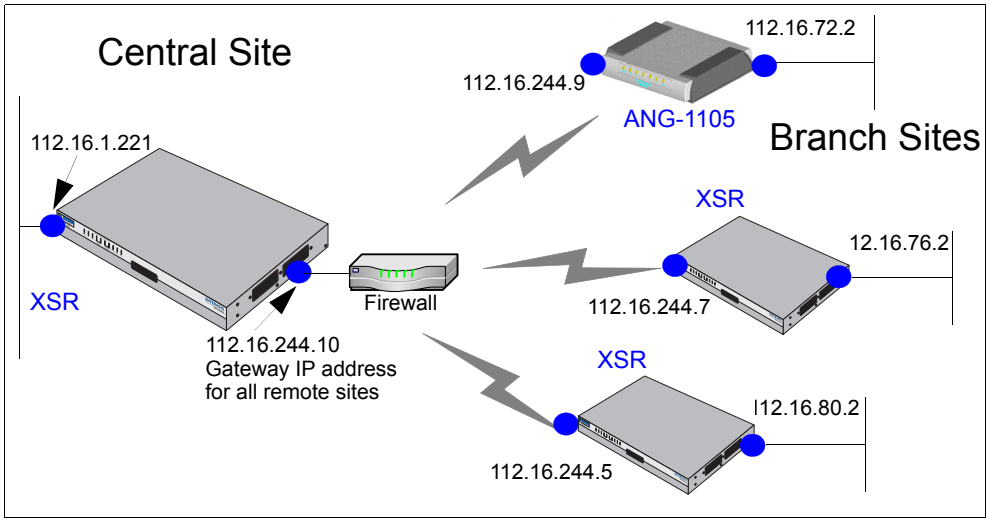
```
XSR(config)#snmp-server host 192.168.2.101 traps trapCommunity
```
+ *Specifies management station to send traps to*

```
XSR(config)#snmp-server host 192.168.2.102 traps trapCommunity
```
+ *Specifies another management station to send traps to*

VPN Site-to-Site Sample Configuration

The following VPN topology, shown in Figure 3-5, configures a central site XSR to connect over IPSec tunnels with a remote ANG-1105 and two XSRs.

Figure 3-5 VPN Site-to-Site Topology



The following script configures the VPN topology shown in Figure 3-5.

Generate Master Encryption Key

If you have not already generated a master encryption key, you must do so now to configure the VPN. A master key need only be generated once.

Caution: The master encryption key is stored in hardware, not Flash, and you cannot read the key - only overwrite the old key by writing a new one. To ensure router security, it is critical not to compromise the key. There are situations where you may want to keep the key, for example, to save the user database off-line in order to later download it to the XSR. In order to encrypt the user database, you need the same master key, indicating the key designation with the master key specify command. Be aware that if the XSR is inoperable you may have to return to factory defaults, which erases the master key forcing you to generate a new one.

Generate the master key:

```
XSR(config)#crypto key master generate

New key is 2173 4521 3764 2ff5
             163b 4bdf fe92 dbc1
             1232 ffe0 f8d9 3649
```

Configure Access Control Lists

ACL 101 configured below is strongly restrictive in denying all but IKE traffic (*well-known* ACL # 500) through the router. ACLs 190, 191, and 192 are crypto map filters configured to accept any IPSec-encrypted traffic over site-to-site tunnels and pass that traffic to the three specified networks only.

```
XSR(config)#access-list 101 permit udp any any eq 500
XSR(config)#access-list 101 permit udp esp any any
XSR(config)#access-list 101 permit udp ah any any
XSR(config)#access-list 101 deny ip any any
XSR(config)#access-list 190 permit ip any 112.16.72.0 0.0.0.255
XSR(config)#access-list 191 permit ip any 112.16.76.0 0.0.0.255
XSR(config)#access-list 192 permit ip any 112.16.80.0 0.0.0.255
```

Set Up IKE Phase I Security

The following proposal sets pre-shared authentication and MD5 hashing:

```
XSR(config)#crypto isakmp proposal acme
XSR(config-isakmp)#authentication pre-share
XSR(config-isakmp)#hash md5
```

Configure IKE Policy for Remote Peer

The following proposal specifies the XSR's remote peer IP address as *any peer* matching its IKE policy, sets NAT to *automatically* detect routers performing NAT between tunnel endpoints and directs the XSR to switch on UDP encapsulation when found.

It also designates the peer as a *gateway* which will initiate the configuration mode in terms of IKE negotiation:

```
XSR(config)#crypto isakmp peer 0.0.0.0 0.0.0.0
XSR(config-isakmp-peer)#proposal acme
XSR(config-isakmp-peer)#config-mode gateway
XSR(config-isakmp-peer)#nat-traversal automatic
```

Create a Transform Set

The following transform-set specifies the specified encryption/data integrity choices, *768-bit* Diffie-Hellman, and an SA lifetime expressed in *kilobytes*. The SA *seconds* lifetime value is disabled. Some commands are abbreviated.

```
XSR(config)#crypto ipsec tra esp-3des-sha esp-3des esp-sha-hmac
XSR(cfg-crypto-tran)#set pfs group1
XSR(cfg-crypto-tran)#set sec lifetime kilobytes 100000
XSR(cfg-crypto-tran)#no set sec lifetime seconds
```

Configure Crypto Maps

The following IKE policy crypto maps are each linked to the earlier added transform-set with matching ACLs and are set by default for the more stringent *tunnel mode*. Maps 91 and 92 match the remote XSRs and map 90 correlates with the ANG. Crypto map statements render the associated ACLs bi-directional.

```
XSR(config)#crypto map acme 92
XSR(config-crypto-m)#set transform-set esp-3des-sha
XSR(config-crypto-m)#match address 192
XSR(config-crypto-m)#set peer 112.16.244.5

XSR(config)#crypto map acme 91
XSR(config-crypto-m)#set transform-set esp-3des-sha
XSR(config-crypto-m)#match address 191
XSR(config-crypto-m)#set peer 112.16.244.7

XSR(config)#crypto map acme 90
XSR(config-crypto-m)#set transform-set esp-3des-sha
XSR(config-crypto-m)#match address 190
XSR(config-crypto-m)#set peer 112.16.244.9
```

Configuring VPN at Interface Mode and Setting Up RIP

The following commands configure the LAN physical ports as follows: GigabitEthernet port 1 is designated *Internal LAN*, with the specified IP address/subnet as the designated network. GigabitEthernet port 2 is named *VPN Cloud,* assigned crypto map *acme* with associated ACLs, and directed not to transmit or receive RIP updates. Also, RIP routing and four IP routes are configured as well as a VPN interface for AAA service.

```
XSR(config)#interface gigabitethernet 1
XSR(config-if<G1>)#description "Internal LAN"
XSR(config-if<G1>)#no shutdown
XSR(config-if<G1>)#ip address 112.16.1.221 255.255.255.0

XSR(config)#interface gigabitethernet 2
XSR(config-if<G2>)#crypto map acme
XSR(config-if<G2>)#description "VPN Cloud"
XSR(config-if<G2>)#no shutdown
XSR(config-if<G2>)#ip access-group 101 in
XSR(config-if<G2>)#ip access-group 101 out
XSR(config-if<G2>)#ip address 112.16.244.10 255.255.255.0
```

```
XSR(config)#interface vpn 57 multi-point
XSR(config-int-vpn)#ip address 192.168.2.1 255.255.255.0

XSR(config)#router rip
XSR(config-router)#network 112.16.10.0
XSR(config-router)#passive-interface gigabitethernet 2
XSR(config-router)#no receive-interface gigabitethernet 2
XSR(config-router)#distribute-list 1 out vpn 1

XSR(config)#ip route 0.0.0.0 0.0.0.0 112.16.244.9
XSR(config)#ip route 112.16.72.0 255.255.255.0 112.16.244.9
XSR(config)#ip route 112.16.76.0 255.255.255.0 112.16.244.7
XSR(config)#ip route 112.16.80.0 255.255.255.0 112.16.244.5
```

Configuring Authentication (AAA)

Configure an AAA user and DEFAULT AAA group for remote users. When an ANG tunnels into the XSR, it will be assigned dynamically to the IP pool *AUTH*. Be aware that groups must be created before users can be added to them. Remember to create the same users and passwords on the ANG. The IP address assigned to the AAA user is the remote gateway IP address.

```
XSR(config)#ip local pool AUTH 192.168.2.0 255.255.255.0
XSR(config)#aaa user 112.16.244.9
XSR(aaa-user)#password dribble
XSR(aaa-user)#group DEFAULT
XSR(aaa-group)#pptp encrypt mppe auto
XSR(aaa-group)#ip pool AUTH
XSR(aaa-group)#policy vpn
```

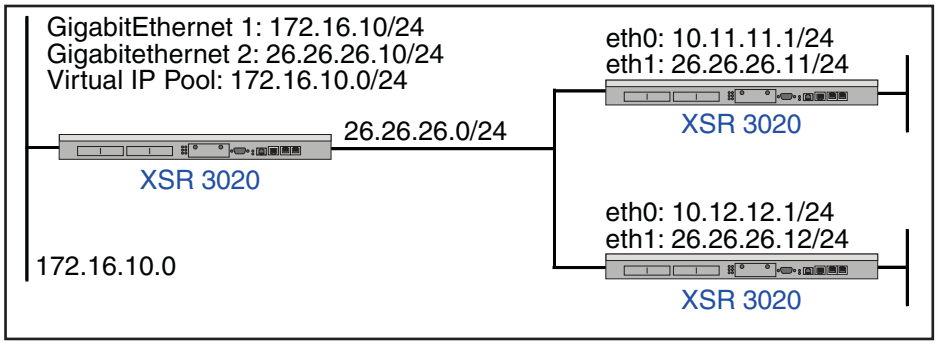
VPN Sample Configuration with Network Extension Mode

The following sample topology is ideal for testing a VPN NEM tunnel connection on a LAN before actually configuring a production network. If the configuration works properly, simply change the GigabitEthernet settings to the Serial or T1 interface values of your choice.

The XSR below is configured as a VPN concentrator with Internet access allowed and Network Extension Mode (NEM) tunnels set up. NEM is designed to open up network resources situated behind the XSR. You configure NEM to provide routing for nodes connected to the trusted port of the router so that locally and remotely connected devices can discover and communicate with each other across an IKE/IPSec tunnel.

The XSR's EZ-IPSec functionality is employed to automatically access default ESP transforms and IPSec proposals. The following script configures the VPN topology shown in Figure 3-6.

Figure 3-6 VPN Topology with NEM, EZ-IPSec and Internet Access



If you have not already generated a master encryption key, you must do so now to configure the VPN. A master key need only be generated once.

Caution: The master encryption key is stored in hardware, not Flash, and you cannot read the key - only overwrite the old key by writing a new one. To ensure router security, it is critical not to compromise the key. There are situations where you may want to keep the key, for example, to save the user database off-line in order to later download it to the XSR. In order to encrypt the user database, you need the same master key, indicating the key designation with the master key specify command. Be aware that if the XSR is inoperable you may have to return to factory defaults, which erases the master key forcing you to generate a new one.

Generate the master key. Refer to the following sample key:

```
XSR(config)#crypto key master generate

New key is 2173 4521 3764 2ff5
           163b 4bdf fe92 dbc1
           1232 ffe0 f8d9 3649
```

Apply the following ACLs to the public interface of the XSR before creating the VPN configuration. These ACLs are applied only to an XSR configured to terminate Network Extension Mode (NEM) tunnels initiated from ANG-1100s. These ACLs allow all outbound IP traffic and established inbound TCP traffic and employ well-known protocol numbers for IKE UDP (500) and ICMP to and from the public interface (if preferred).

```
XSR(config)#access-list 1 deny 26.26.26.0 0.0.0.255
XSR(config)#access-list 1 permit any
XSR(config)#access-list 110 permit udp any any eq 500
XSR(config)#access-list 110 permit icmp any host 26.26.26.10
XSR(config)#access-list 110 deny ip any any

XSR(config)#access-list 111 permit udp any any eq 500
XSR(config)#access-list 111 permit icmp host 26.26.26.10 any
XSR(config)#access-list 111 deny ip any any

XSR(config)#interface gigabitethernet 2
XSR(config-if<G2>)#ip access-group 110 in
XSR(config-if<G2>)#ip access-group 111 out
```

Enable Network Address Translation:

```
XSR(config-if<G2>)#ip nat source assigned overload
```

Create the VPN virtual subnet:

```
XSR(config)#ip local pool virtual_subnet 10.10.10.0 255.255.255.248
```

Configure AAA authentication by assigning a virtual subnet to the DEFAULT AAA group, associate it with DNS and WINs servers, and add two AAA users with passwords.

When a remote XSR tunnels into the local XSR, it will be assigned these DNS, WINS and PPTP values and be assigned dynamically to the IP pool *virtual_subnet*. Be aware that users not added to a specified group will automatically be assigned to the DEFAULT group and groups must be created before users can be added to them. Remember to create the same users and passwords on the remote XSRs.

```
XSR(ip-local-pool)#aaa group DEFAULT
XSR(aaa-group)#ip pool virtual_subnet
```

Configure DNS and WINS parameters:

```
XSR(aaa-group)#dns server primary 172.16.10.10
XSR(aaa-group)#dns server secondary 172.16.10.11
XSR(aaa-group)#wins server primary 172.16.10.10
XSR(aaa-group)#wins server secondary 172.16.10.11
```

Create user(s), specify an IP from virtual subnet, and assign a password:

```
XSR(config)#aaa user nem-test
XSR(config)#password welcome
XSR(config)#aaa user jeffb
XSR(config)#password welcome
```

Check to make sure the transforms and proposals were created properly:

```
Router#show crypto ipsec transform-set
 Name                      PFS       ESP      ESP-AH     AH  IPCOMP
 ----                      ---       ---      ------     --  ------
*ez-esp-3des-sha-pfs       Modp768   3DES     HMAC-SHA   None       None
*ez-esp-3des-sha-no-pfs    Disabled  3DES     HMAC-SHA   None       None
*ez-esp-3des-md5-pfs       Modp768   3DES     HMAC-MD5   None       None
*ez-esp-3des-md5-no-pfs    Disabled  3DES     HMAC-MD5   None       None
*ez-esp-aes-sha-pfs        Modp768   AES      HMAC-SHA   None       None
*ez-esp-aes-sha-no-pfs     Disabled  AES      HMAC-SHA   None       None
*ez-esp-aes-md5-pfs        Modp768   AES      HMAC-MD5   None       None
*ez-esp-aes-md5-no-pfs     Disabled  AES      HMAC-MD5   None       None

XSR#show crypto isakmp proposal
 Name                 Authentication  Encrypt  Integrity  Group     Lifetime
 ----                 --------------  -------  ---------  -----     --------
*ez-ike-3des-sha-psk  PreSharedKeys   3DES     HMAC-SHA   Modp1024     28800
*ez-ike-3des-md5-psk  PreSharedKeys   3DES     HMAC-MD5   Modp1024     28800
*ez-ike-3des-sha-rsa  RSASignature    3DES     HMAC-SHA   Modp1024     28800
*ez-ike-3des-md5-rsa  RSASignature    3DES     HMAC-MD5   Modp1024     28800
```

Create the ISAKMP IKE global peer:

```
XSR(config)#crypto isakmp peer 0.0.0.0 0.0.0.0
XSR#config)#config-mode gateway
XSR(config)#exchange-mode aggressive
XSR(config)#proposal ez-ike-3des-sha-psk ez-ike-3des-md5-psk
```

Create the ACL for trusted subnet of the XSR and virtual subnet of XSR:

```
XSR(config)#access-list 101 permit ip any 10.11.11.0 0.0.0.255
XSR(config)#access-list 102 permit ip any 10.12.12.0 0.0.0.255
```

```
XSR(config)#access-list 103 permit ip any 10.10.10.0 0.0.0.255
```

Create crypto map statements for each ACL entry with the more protective *tunnel* mode set by default. *Match* statements render associated ACLs bi-directional:

```
XSR(config)#crypto map test 101
XSR(config)#set transform-set ez-esp-3des-sha-pfs
XSR(config)#match address 101

XSR(config)#crypto map test 102
XSR(config)#set transform-set ez-esp-3des-sha-pfs
XSR(config)#match address 102

XSR(config)#crypto map test 103
XSR(config)#set transform-set ez-esp-3des-sha-pfs
XSR(config)#match address 103
```

Create the multi-point VPN virtual port required to terminate many clients:

```
XSR(config)#interface vpn1 multi-point
XSR(config)#description "VPN Virtual Interface Int0"
XSR(config)#ip address 10.10.10.1 255.255.255.0
XSR(config)#ip rip send version 2
XSR(config)#ip rip receive version 2
XSR(config)#ip multicast-redirect tunnel-endpoint
```

Enable RIP routing on all networks *except* the public interface:

```
XSR(config)#router rip
XSR(config)#network 172.16.10.0
XSR(config)#network 10.0.0.0
XSR(config)#passive-interface gigabitethernet2
XSR(config)#no receive-interface gigabitethernet2
XSR(config)#distribute-list 1 out vpn1
```

Finally, attach the crypto map statement to the public interface:

```
XSR(config)#interface gigabitethernet 2
XSR(config-if<G2>)#crypto map test
XSR(config-if<G2>)#end
XSR#copy running-config startup-config
```

XSR Rebooting Characteristics

When the XSR reboots, it conforms to the behavior described in this section. The output displayed at the CLI describes router initialization.

Initialization Output

The XSR displays the following output when it initializes (cold reboot):

The XSR displays the following output when it initializes (cold reboot):

```
X-Pedition Security Router Bootrom
Copyright 2003 Enterasys Networks Inc.

HW Version: 9002914-04 REV0A  Serial Number: 3646031700233215
```

```
CPU: Broadcom BCM1250 Rev 2
VxWorks version: VxWorks5.4.2
Bootrom version: 1.5
Creation date: Aug 26 2003, 10:12:36

Warm Start : from cli

Testing Bootrom Integrity << PASSED >>

auto-booting...

Verifying flash:xsr3000.fls file ...
Router S/W size=11989192 sum=0xedd1 compressed_size=4109639 entry=0x80020000
Diagnostics size=1459880 sum=0x8154 compressed_size=614417 entry=0x80020000
RouterCpu1 S/W size=1520104 sum=0x4a2c compressed_size=652528 entry=0x82020000
Testing S/W Integrity << PASSED >>
Loading Router S/W to address 0x80020000

Verifying uncompressed chksum ...
Starting from 0x80020000...

Attaching shared memory objects at 0xa0000600... done
Attaching interface lo0...done
Verifying flash:xsr3000.fls file ...
Router S/W size=11989192 sum=0xedd1 compressed_size=4109639 entry=0x80020000
Diagnostics size=1459880 sum=0x8154 compressed_size=614417 entry=0x80020000
RouterCpu1 S/W size=1520104 sum=0x4a2c compressed_size=652528 entry=0x82020000
Testing S/W Integrity << PASSED >>
Cpu1 software loaded at address 0x82020000, size is 0x001731e8


==cpu1:Running.

********************* REMOTE AUTO INSTALL STARTING ************************

Remote Auto Install Terminating - No Serial Cards Installed
login:
```

Reboot Triggers

Although there are two types of reboots of the XSR - warm or cold - reboots can be triggered in up to eight different ways. Refer to the table below.

Table 1 Reboot Triggers

Cause	Boot Type
Power-up	Cold
CLI reload	Cold or Warm

Table 1 Reboot Triggers (continued)

Cause	Boot Type
SNMP reload	Cold or Warm
Watchdog Expiration	Warm
Software Crash	Warm
Repetitive Software Crash	Cold
ROM Monitor	Cold or Warm
Invalid SW text checksum	Warm

Power-Up Reboot

If you power cycle the XSR by flipping the switch on the back panel, the XSR will cold reboot. The **`startup-config`** file stored in Flash becomes the running configuration.

Reload Command from the CLI

You can reboot the XSR firmware by issuing the command **`reload <cold | warm>`**. You are then prompted to confirm the command. Once the firmware is reloaded, the configuration is loaded from the startup-config file.

Bootrom Monitor Commands bc and bw

Using Bootrom Monitor mode, you can activate warm or cold reboots by entering **`bw`** or **`bc`**, respectively. Refer to "Bootrom Monitor Mode Commands" on page 3-35 for more data.

Watchdog Timer Expiration

When the internal watchdog timer expires, causing the XSR to fail, fault information is captured in a report and a warm boot is initiated. But if more than three warm boots are detected within one minute, a cold boot will be initiated.

System Crash

When system exceptions occur causing the XSR to fail, fault information is captured in a report and a warm boot is initiated. But if more than three warm boots are detected within one minute, a cold boot will be initiated.

Restart with Default Configuration Interrupt

When you press the Default button on the back panel, the XSR restarts using factory default parameters, ignoring the **`startup-config`** file.

Power-up Error Conditions

After power-up, the XSR comes up automatically if:

- The minimum hardware is functional: Processor, RAM and FLASH memory, and other components.

- Bootrom is valid.
- The software image in Flash is valid.

Bootrom Monitor Mode Commands

Bootrom monitor mode offers special user access when the XSR lacks valid software or runs abnormally. Enter the mode by pressing the key combination (**CTRL-C**) during the first five seconds of initialization. After you access the mode, list command groups by typing **h** to show the text below:

```
b      Boot
f      Files
n      Network
s      Status
t      Time and Date
D      For Development Only
```

All the commands in each group can be listed by entering the command group letter. The main menu provides the following functions:

- Reboot warm or cold
- Update Bootrom
- File system-related commands for the Flash ROM file system
- Modify network parameters
- Various status/show commands
  - Version number
  - Hardware information
  - Display crash info
- Display or change date and time on real-time clock if present
- Commands for development use only

Caution: Upon accessing Bootrom monitor mode, if you do not provide the password (if configured earlier with the **bp** command) when prompted or enter an incorrect password five times, the XSR will delete your configuration and reinstitute factory default settings. This function is similar to pressing the reset button on the XSR-1800 Series routers.

bc

This command initiates a *cold* reboot.

bw

This command initiates a *warm* reboot.

bp

This command changes the Bootrom password. The default password is blank. You are prompted to enter a password by the following script:

```
XSR-3020:bp
Enter current password:
Enter new password: ******
Re-enter new password: ******
Password has changed.
```

bu

This command updates the bootrom from a local file. You are prompted to enter data by the following script. When the "**Proceed with erasing Bootrom in flash** ..." statement appears, enter **y**. Be sure not to interrupt the process or power down the XSR or it may be affected adversely. After you have updated this file, you can delete it from Flash to conserve space for other files.

```
XSR-3020: bu btXSR3000_1_2.fls
Verifying btXSR3000_1_2.fls file ...
bootFirst size=28992 sum=0xc2e5 compressed_size=28992 entry=0x80020000
bootrom size=842656 sum=0xfa65 compressed_size=347728 entry=0x81e00000
OK

Proceed with erasing current Bootrom in flash and replace with btXSR3000_1_2.fls?
(y/n) y

First copy of Bootrom ...
Erasing 3 sectors at address=0xbfc20000
Programming 131072(0x20000) bytes at address 0xbfc20000
Programming 131072(0x20000) bytes at address 0xbfc40000
Programming 85600(0x14e60) bytes at address 0xbfc60000
Verifying Bootrom flash sectors
Locking 3 Bootrom flash sectors

Second copy of Bootrom ...
Erasing 3 sectors at address=0xbfca0000
Programming 131072(0x20000) bytes at address 0xbfca0000
Programming 131072(0x20000) bytes at address 0xbfcc0000
Programming 85600(0x14e60) bytes at address 0xbfce0000
Verifying Bootrom flash sectors
Locking 3 Bootrom flash sectors

*****   Bootrom update completed.   *****
```

bU

This command updates the bootrom through a network transfer to a local file. Be sure to enter the **U** in uppercase. After you have updated this file, you can delete it from Flash to conserve space for other files.

cd

This command changes the current directory in the file system to **flash:** or **cflash:**.

copy

This command copies a file using the syntax **copy <source name> <destination name>**. You can copy files from *flash:* to *cflash:* and vice versa.

da

This command shows system date/time with the sample output below:

```
XSR-3020:da
Date: Thursday, 29-MAY-2003.
Time: 10:14:07
```

df

This command shows free disk space. Sample output is shown as follows:

```
XSR-3020: df
Free space on flash: is 3383296 bytes (0x33a000).
```

del

This command removes a file from **flash:** or **cflash:** memory.

dir

This command lists the contents of the current directory in long format. The command displays the following sample output:

```
XSR-3150: dir


Listing Directory flash::
-rwxrwxrwx  1 0       0          4678118 May  5 23:06 xsr3000.fls
-rwxrwxrwx  1 0       0             2228 May 29 09:57 persistent-data
-rwxrwxrwx  1 0       0             1153 May 29 09:51 startup-config
-rwxrwxrwx  1 0       0                0 May 29 09:51 private-config

    2895872(0x2c3000) bytes free on flash:
```

ds

This command sets the system date with the syntax **yyyy mm dd w (1=Sunday)**. For example:

```
XSR-3020: ds 2003 6 1 3
```

dt

This command sets the system time using the syntax **hh mm ss**. E.g.:

```
XSR-3020: ds 11 59 59
```

ff

This command formats the Flash file system. We recommend that you first save any **.dat, .cert, .cfg**, and your **startup-config** files to **cflash:** or a PC since any files in **flash:** will be deleted. You are prompted to enter data by the following script:

```
XSR-3020: ff
You will lose all files in the "flash:" file system.
Are you sure you want to format the "flash:" file system? (y/n) y
Unlocking flash file sectors
Initializing DOS file system.
Formatting flashrom file system
.................................................. Done.
Set working directory to flash:

Using default Bootrom password. The system is not secure!!!
Use "bp" to change password
```

ffc

This command formats the CompactFlash card.

ng

This command retrieves a file over the network using a remote IP address/file path.

np

This command modifies network parameters. You are prompted to enter data by the following script. While most of the options are self-explanatory, three require further description.

- When set to *no*, the *Autoboot* option places the prompt in Bootrom mode when you boot or power up the XSR.
- When set to *yes*, the default *Quickboot* action of delaying five seconds at startup for you to optionally enter CTRL-C and acquire Bootrom mode is negated. You can still acquire Bootrom mode, but you must immediately press CTRL-C upon seeing the *X-Pedition Security Router Bootrom* header.
- The default hostname (local target name), *XSR-3000*, cannot be changed. In the absence of a user-supplied hostname via the **hostname** CLI command, this name will be used as the CLI prompt and SNMP hostname in MIB-II.

```
XSR-3020: np

Enter '.' = clear a field; '-' = go to previous field;  ^C = quit

Local IP address    (192.168.1.1)       :
Gateway IP address                ()    :
Remote Host IP address (192.168.1.10)   :
Remote file path (c:\)                  :
Use TFTP (no)                           :
Ftp userid (anonymous)                  :
Ftp password ()                         :
```

```
Local target name (robo1)               :
Autoboot (yes)                          :
Quick boot (no)                         :

Permanently save the network parameters? (y/n)
```

ns

This command saves a file over the network using a remote IP address/file path.

remove

This command removes a file using the syntax **`remove <source name> <destination name>`**

rename

This command renames a file using the syntax **`rename <source name> <destination name>`**

sb

This command displays boot values. Sample output is shown as follows:

```
XSR-3020: sb
Current boot file is xsr3000.fls
Boot selector default is flashrom, compactFlash, network
Available Network boot devices: sbe0
```

sf

This command displays a fault report. Sample output is shown as follows. You can enter **`sf`** to display output from both CPUs or **`sf 0`** or **`sf 1`** to display output from either CPU.

```
XSR-3020: sf

Software Revision: 6.0.0.0 without VPN; without Firewall
Creation Date:     Sep  7 2003, 16:07:42
Broadcom BCM1250 Rev 2 CPU0 up-time 0 hours 2 minutes 20 seconds
Crashed Task = PP, Task Status = 0, errno=0 initStage=0
Exception Vector Number=0x5, Address error exception, store
pc=      821014b0  sp=     85febb90  STATUS=  3400ff81
zero=    00000000  at=      08110000  v0=      11223344   v1=      00000000
a0=      3400ff81  a1=      00000000  a2=      3400ff81   a3=      85feb8f8
t0=      00000000  t1=      3400ff80  t2=      3400ff81   t3=      00000000
t4=      00000001  t5=      0000009b  t6=      0a0122d4   t7=      00000004
s0=      85febbe0  s1=      8219d3dc  s2=      00000000   s3=      00000000
s4=      00000000  s5=      00000000  s6=      00000000   s7=      00000000
t8=      00000000  t9=      00080000  k0=      eeeeeeee   k1=      00000000
gp=      8219b1e0  sp=      85febb90  s8=      00000000   ra=      820e9178
par1=    ffffffff  par2=    85febaf8  par3=    ffffffff   par4=    820e9b10
cause=   80000014  cntxt=   ffffffff  fpcsr=   d3800000   badva=   08112233
divLo=   00000000  divHi=   00000000 causeR=  ffffffff   fpcsr=   820e9170
```

```
BadVAddr=08112233

PP - Crashed Task Stack (sp=85febb90):
0x85feb790    ffffffff  00000000  00000008  ffffffff
0x85feb7a0    00000000  00000001  00000000  00000001
0x85feb7b0    00000000  8214ab00  0000000a  82142ee0
0x85feb7c0    ffffffff  85feb7c0  ffffffff  bf3285a4
0x85feb7d0    00000000  00000002  ffffffff  85feb7e0
0x85feb7e0    ffffffff  82154b50  00000000  00000017

......
```

si

```
This command displays XSR 3000 Series inventory with this sample output:
XSR-3020: si
Hardware:
   Motherboard Information:
   XSR-3250 ID: 9002914-04 REV0A CPLD Rev 3
    Serial Number: 2914024201123206
    Processor: Broadcom BCM1250 Rev 2 at 600MHz
    PowerSupply1, PowerSupply2
   Fans 1 2 3 4 5 7 8 10
    CPU Temperature Max: 80C  Current: 35C
    Router Temperature Max: 60C  Current: 23C
    RAM: 512MB without interleave
       Memory Bus at 120MHz, CASL at 2.0
   Bootrom Flash: 4MB
   Filesystem Flash: 8MB
   CompactFlash not present
    Real Time Clock
   I/O on Motherboard:
   GigabitEthernet  1 2 3
    Encryption Hardware: not present
    Slot 0 card 1: Empty
    Slot 0 card 2: Empty

   System up for 9 days, 3 hours, 4 minutes 10 seconds.
```

sn

This command shows network values with the following sample output:

```
XSR-3020: sn

Local IP address   : 192.168.1.12
Gateway IP address : 192.168.1.1
Remote IP address  : 192.168.1.2
Remote file path   : c:/XSR3000
Transfer Protocol  : FTP
```

```
Local target name  : XSR1
Autoboot           : enabled
Quick boot         : no

Current GigabitEthernet 0 MAC address is: 00:01:f4:2b:3e:1b
Current GigabitEthernet 1 MAC address is: 00:01:f4:2b:3e:1c
Current GigabitEthernet 1 MAC address is: 00:01:f4:2b:3e:1d
```

sv

This command shows the bootrom version with sample output below:

```
XSR-3020: sv

                  X-Pedition Security Router Bootrom
                  Copyright 2003 Enterasys Networks Inc.

HW Version: 9002914-04 REV0A  Serial Number: 3646031700233215
CPU: Broadcom BCM1250 Rev 2
VxWorks version: VxWorks5.4.2
Bootrom version: 1.0
Creation date: Apr 14 2003, 10:12:36
```

A

Specifications

System Specifications

This appendix details XSR data about hardware functionality including:

- Processor, system memory, chassis, power supply, interfaces
- Required cabling, optional CompactFlash and other accessories
- Pinout assignments for WAN and LAN interfaces
- LED behavior

Refer to tables throughout this appendix for specific information.

Table A-1 XSR Hardware Specifications

Category		Parameters
Processor	Type	Broadcom 1250 with two CPU cores
	Dual-core Operating Speed	1700 Dhrystone MIPS @ 600 Mhz
Hardware accelerator	VPN	Encryption Module chip (310 Mbps) for 3DES encryption, message digest (MD-5, SHA-1), public key acceleration
System Memory	RAM	Micron 184-pin, SDRAM DIMM, 128 Mbyte memory modules at 133 MHz (total 256 MBytes)
	Non-Volatile	8 Mbytes of Onboard Flash - no upgrade
		Up to 1 Gbyte optional plug-in CompactFlash card. Type I and II CF cards supported
Chassis	Form Factor	19-inch rack-mountable
	Dimensions	1U (1-11/16 inches high by 17 inches wide by 21 inches deep)
	Weight	17 pounds
Heat Dissipation	Forced air cooling	Maximum heat release of a fully configured system is 443.3 BTU/hr
Environment	Operating temp.	0 - 40° C
	Storage temp.	-40 - 70° C
	Relative Humidity	5% - 90%, non-condensing

Table A-1 XSR Hardware Specifications (continued)

Category		Parameters
Power Consumption	Typical values:	Motherboard: 75 watts (maximum) Serial NIM card: 4 watts T1/E1/ISDN-PRI NIM card: 3 watts ISDN BRI-S/T NIM card: 1 watt
Internal Power Supply	Type	Universal (110/220 VAC) unit
	Input AC Voltage & Frequency	100-125 Vac, 1.25A 200-240 Vac, 0.65A 50/60Hz
I/O Interfaces	Onboard (LAN)	2 10/100/1000Base-T Ethernet ports with RJ-45 copper connectors, and 10/100/1000 or Mini-GBIC optical connector
		RS-232 COM (console) serial port with DB-9 connector
I/O Interfaces	NIM (WAN)	Dual or Quad synch/asynch Serial ports with DB-type connector also supporting X.21, V.35, EIA-449, EIA-232/530 and combined V.35/EIA-232/530 DTE interfaces with required adapter.
		Single, dual, or quad T1/E1 RJ-48C port(s) with integral CSU/DSU. Full-channel, fractional or unchannelized.
		Single port T3/E3 un-channelized NIM with BNC connectors
I/O Interfaces	NIM (WAN)	Dual or quad port BRI/PRI S/T NIM (RJ-45) or U NIM with RJ-45 or RJ-49C connectors, respectively.
		Single port Annex A/C or B ADSL NIM with RJ-11 connector. Includes CompactFlash card.
		Dual port T1/E1 Drop and Insert NIM with RJ-45 connectors.
	NIM (LAN or WAN)	Single port 10/100Base-T Copper or 10/100Base-F Fiber-optic Ethernet NIM with RJ-45 connector or MT-RJ multi-mode interface, respectively.
Chassis LEDs	14	Display port and system status, warn of Flash upgrade

Cable, CompactFlash and Accessory Specifications

Refer to the following table for specifications of cables, CompactFlash and accessories for the XSR. This equipment can all be obtained separately from Enterasys Networks or through any computer supply retailer.

Table A-2 XSR Cabling/Accessory Guide

Part Description	Connector	Part #	Function
6’ DB-9 null modem cable	DB-9, male	N/A from Enterasys	COM link to serial line
.58, 1, 2, 3, 5, or 10 meter 10/100BaseT straight-through or cross-over cable	RJ-45	N/A from Enterasys	Ethernet link to hub/switch or PC/uplink port
1000Base-SX Mini-GBIC with connector 1000Base-LX Mini-GBIC with connector 1000Base-SX Mini-GBIC with connector	Short-haul LC Long-haul LC Short-haul MTRJ	MGBIC-LC01 MGBIC-LC09 MGBIC-MT01	Ethernet link to 1000BaseT line Ethernet link to 1000BaseT line Ethernet link to 1000BaseT line

Table A-2 XSR Cabling/Accessory Guide (continued)

Part Description	Connector	Part #	Function
2-port synch/asynch card 4-port synch/asynch card	68-pin, male SCSI III	NIM-SER-02 NIM-SER-04	Serial NIM cards
6' DB-15, X.21 DTE, twisted-pair cable		NIM-X21-CAB-04	Serial link to high speed serial line: 2 or 4 port
6' DB-25, EIA-232/530 DTE twisted-pair cable		NIM-232-CAB-04	
6' DB-37, EIA-449 DTE, twisted-pair cable		NIM-449-CAB-04	
6' DB-V.35 DTE, twisted-pair cable		NIM-V35-CAB-04	
Combined V.35/EIA-232/530 DTE, twstd-pr cable	68-pin, male SCSI III	NIM-DBU1-CAB-04	Serial link to high speed serial line: 2 or 4 port
-Single unchannelized card -Dual unchannelized card -Quad unchannelized card	RJ48C RJ48C RJ48C	NIM-T1/E1-01 NIM-T1/E1-02 NIM-T1/E1-04	T1/E1 NIM cards
-Single channelized PRI card -Dual channelized PRI card -Quad channelized PRI card	RJ48C RJ48C RJ48C	NIM-CT1E1/PRI-01 NIM-CT1E1/PRI-02 NIM-CT1E1/PRI-04	Single channelized PRI card Dual channelized PRI card Quad channelized PRI card
Single unchannelized T3/E3 card	2 female BNCs	NIM-T3E3-01	Single unchannelized T3/E3 NIM
1-port ISDN BRI-S/T card 2-port ISDN BRI-S/T card	RJ-45 RJ-45	NIM-BRI-ST-01 NIM-BRI-ST-02	BRI-S/T NIM card BRI-S/T NIM card
1-port ISDN BRI-U card 2-port ISDN BRI-U card	RJ49C RJ49C	NIM-BRI-U-01 NIM-BRI-U-02	BRI-U NIM card BRI-U NIM card
1-port Annex A/C ASDL card 1-port Annex B ASDL card	RJ-11 RJ-11	NIM-ADSL-AC-01 NIM-ADSL-B-01	ADSL NIM card ADSL NIM card
2-port T1/E1 D&I card	RJ-45	NIM-DIRELAY-02	T1/E1 D&I NIM card
1-port Copper Ethernet card 1-port Fiber-optic card	RJ-45 MT-RJ	NIM-ETHR-01 NIM-FIBR-01	Copper Ethernet NIM card Fiber-optic Ethernet NIM card
100/120-ohm, straight-thru, twisted-pair cables	T1 or E1Port	N/A from Enterasys	-
75-ohm coaxial to 120-ohm adapter	2 female BNCs & 1 RJ-48C port	9372192	G.703 Balun adapter for E1 line
Grounding shunt	P2 - P5	N/A from Enterasys	Insulator for E1 line
Auxiliary Flash RAM card: 1.4"L x 1.6" W	Front panel slot	N/A from Enterasys	CompactFlash card for greater software storage and flexibility
XSR-3020 Firewall and VPN firmware	-	XSR-3020-VPN-FW	Firewall and VPN code
XSR-3020 VPN firmware	-	XSR-3020-VPN	VPN code
XSR-3020 Firewall firmware	-	XSR-3020-FW	Firewall code

COM (Console) Port

The XSR comes equipped with a COM serial port useful for initial configuration and management.

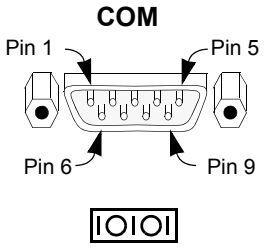
Using a serial (null modem) cable, you can attach the router's DB-9 COM port to a data terminal port and directly configure the XSR over the asynchronous connection. Then, open a communications or Telnet session to communicate with the router. If you use a communications program, set the connection properties as follows:

- Connect using: Direct to COM*x* (where *x* is an unused COM port)
- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: none

Note: The XSR default l login is *Admin* with no password.

Refer to Figure A-1 for pinout assignments.

Figure A-1 COM Port Pinouts



Pin	Signal
1	Carrier Detect (CD)
2	Receive Data (RX)
3	Transmit Data (TX)
4	Data Term Ready (DTR)
5	Ground (GND)
6	Data Set Ready (DSR)
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	Ring Indicator (RI)

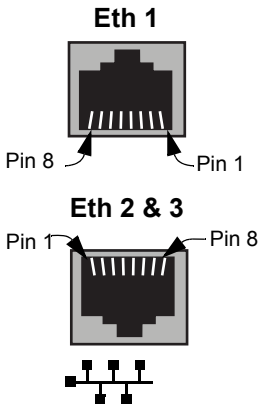
GigabitEthernet Ports

The XSR comes equipped with three GigabitEthernet (LAN) ports that support full-duplex 10, 100, or 1000 Mbps transmission. The ports conform to IEEE 802.3 standards with 8-pin modular RJ-45 connectors. Because these ports have internal MDI crossover capabilities which allow them to detect which mode (DTE or DCE) the link partner is operating at, you can use any cable to attach the XSR with a PC or uplink port as long as a fully populated cable (all four pairs) is connected to take advantage of full gigabit bandwidth.

When GigabitEthernet interface 1 is used, the Mini-GBIC port is unavailable, and vice versa.

Refer to Figure A-2 for pinout assignments.

Figure A-2 GigaBitEthernet Port Pinouts



Pin	Signal
1	TRDO+
2	TRDO-
3	TRD1+
4	TRD2+
5	TRD2-
6	TRD1-
7	TRD3+
8	TRD3-

Mini-GBIC Fiber, Copper Port

The XSR offers a 1000Base-T GigabitEthernet port that supports full or half-duplex 1000 Mbps transmission. The 20-pin, Mini-GBIC socket accepts all SFP MSA compliant Mini-GBIC modules.

Be aware of the following conditions when using Fiber or Copper ports:

- When the Mini-GBIC port is used, GigabitEthernet port 1 is disabled.
- When GigabitEthernet port 1 is used, the Mini-GBIC port is disabled.
- If *both* Fiber and Copper ports are plugged in, only Fiber is enabled.
- On GigabitEthernet port 1, when the far end of the line is active, the Fiber port takes precedence.
- If the Fiber port is connected, **speed** must be set to **auto** to achieve 1000 Mbits.
- If the fiber port is connected, **speed** and **duplex** *must* be set to **auto** on both ends of the line otherwise the connection will be unpredictable.

Refer to the *XSR CLI Reference Guide* for more command details.

Cabling for the Mini- GBIC is supported using an MT-RJ connector with a fiber link or the appropriate connector with a copper link.

Copper/Fiber-optic Ethernet NIMs

The single-port Copper or Fiber-optic Ethernet NIMs, shown in Figure A-3 and Figure A-4, provide interfaces for half and full-duplex 10/100Base-T or fiber-optic 100Base-F transmission over LAN or WAN networks, respectively. The Copper Ethernet NIM incorporates a standard 8-pin modular RJ-45 connector and the Fiber-optic Ethernet NIM has an MT-RJ multi-mode interface. Both NIMs conform to IEEE 802.3 and PCI 2.2 standards.

Figure A-3 Copper Ethernet NIM

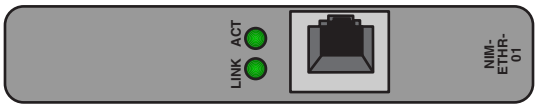
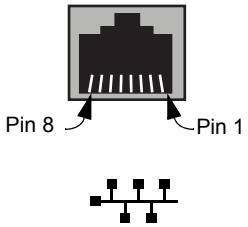


Figure A-4 Fiber-optic Ethernet NIM

Refer to Figure A-5 for Copper Ethernet NIM pinout assignments.

Figure A-5 Copper Ethernet NIM Port Pinouts



Pin	Copper Signal
1	Tx Data +
2	Tx Data -
3	Rx Data +
4	Not Used
5	Not Used
6	Rx Data -
7	Not Used
8	Not Used

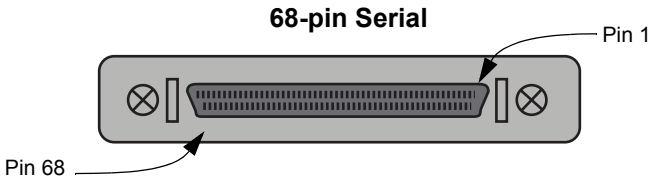
Regulatory/Safety Compliance

The Copper and Fiber-optic Ethernet NIMs comply with these requirements: IEE 802.3, UL 1950, CSA No. 950, EN 60950, and IEC 950 (CB Scheme Report).

2/4-Port Serial NIM Card Port

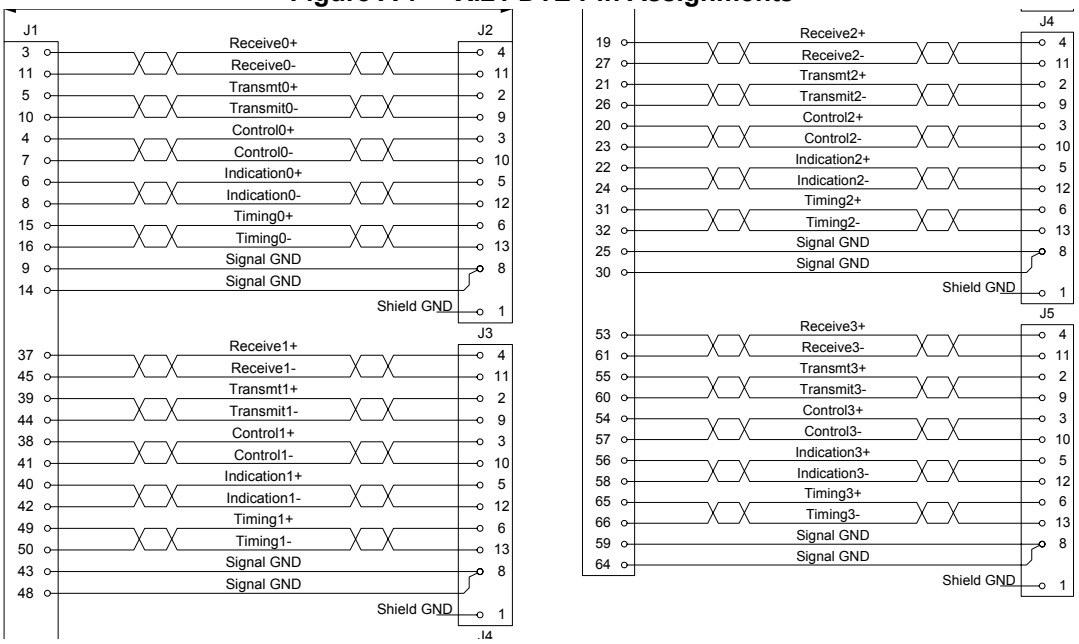
The High Speed Serial NIM card, as shown in Figure A-6, provides a WAN interface supporting a serial link to four different types of DTEs: DB-15, 25, 37, and V.35. This interface supports dual and quad traffic up to 8 Mbps.

Figure A-6 High Speed Serial NIM Port



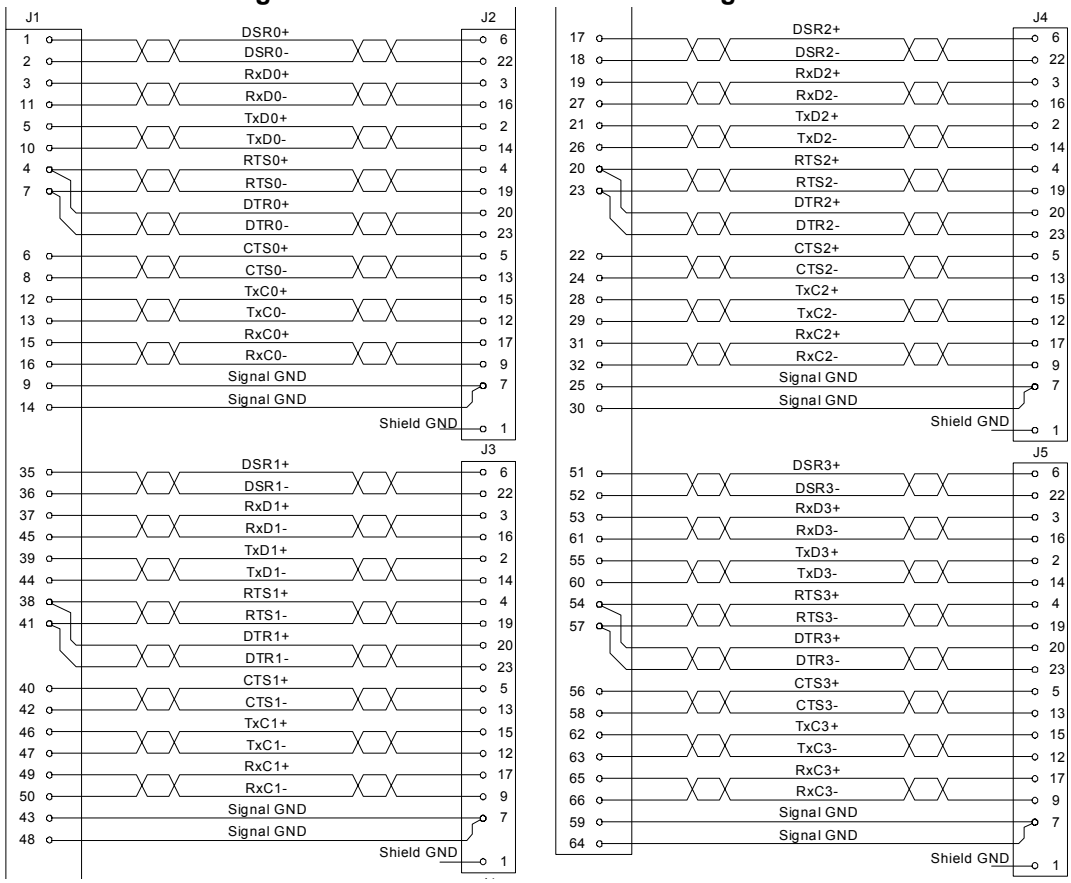
Refer to Figure A-7 through Figure A-11 for pinout assignments.

Figure A-7 X.21 DTE Pin Assignments



J1: 68-pin male SCSI II type connector
J2 - J5: DB-15 type male connector

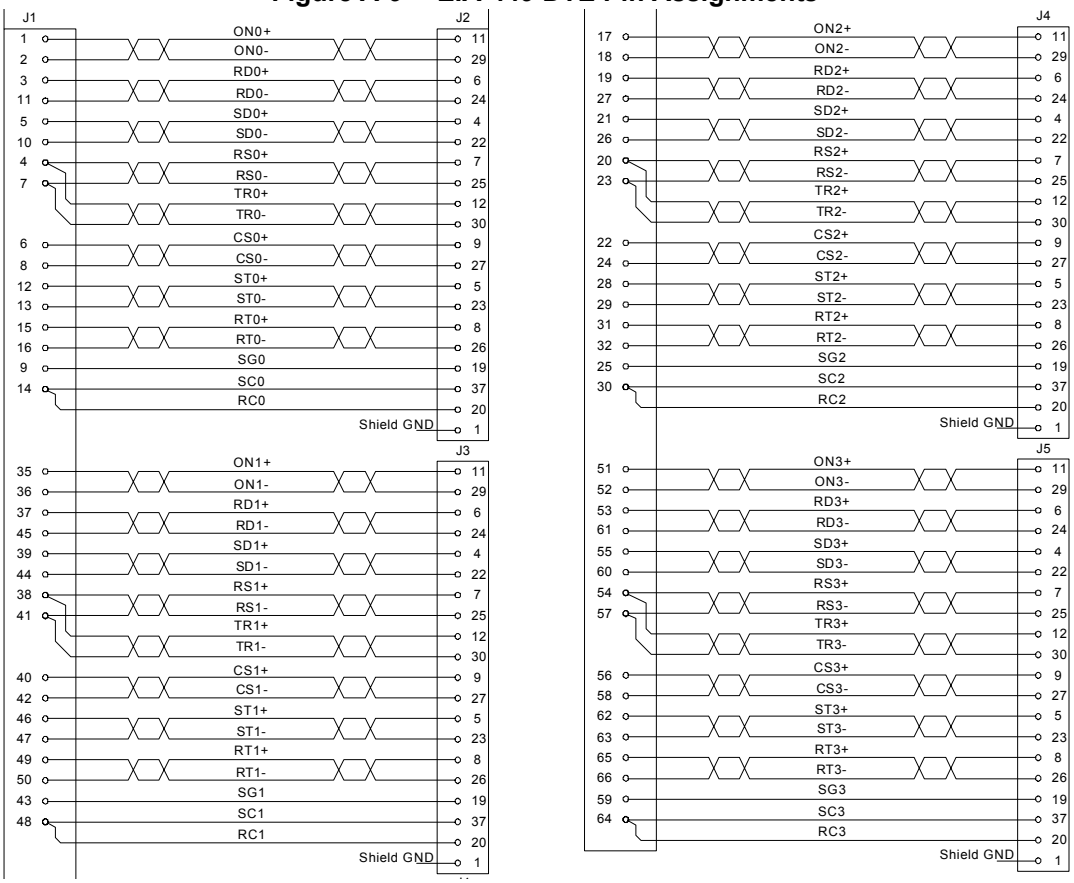
Figure A-8 EIA-232/530 DTE Pin Assignments



J1: 68-pin male SCSI II type connector

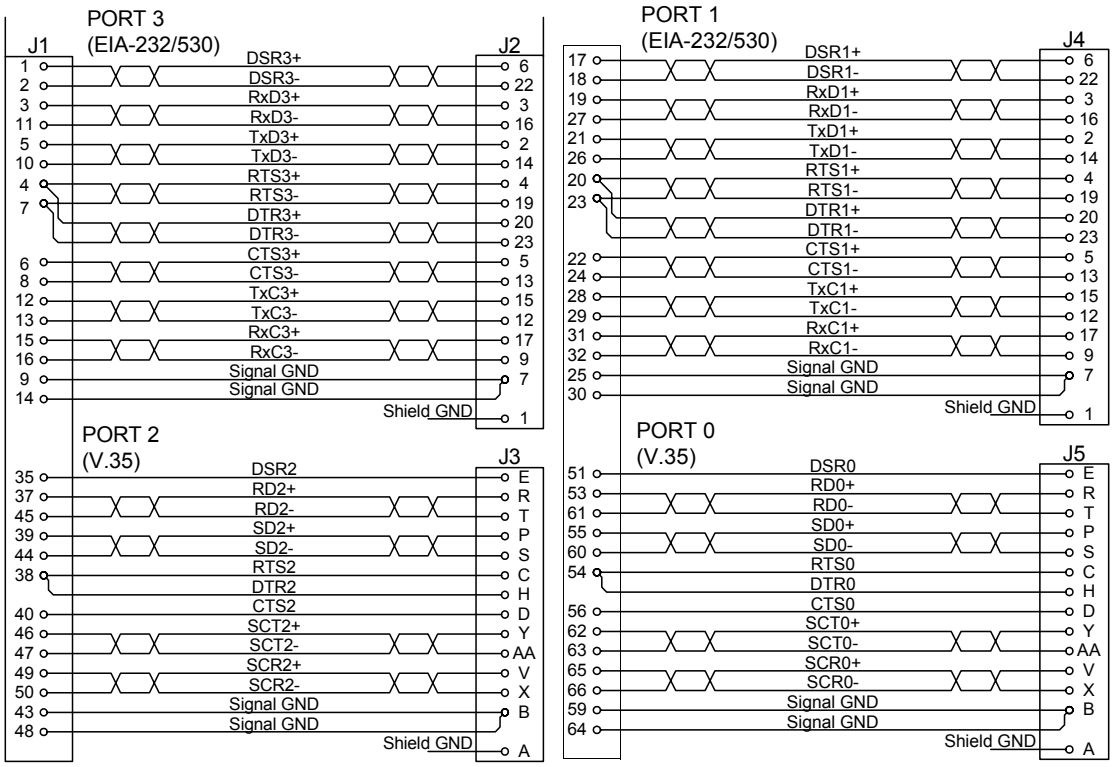
J2 - J5: DB-25 type male connector

Figure A-9 EIA-449 DTE Pin Assignments



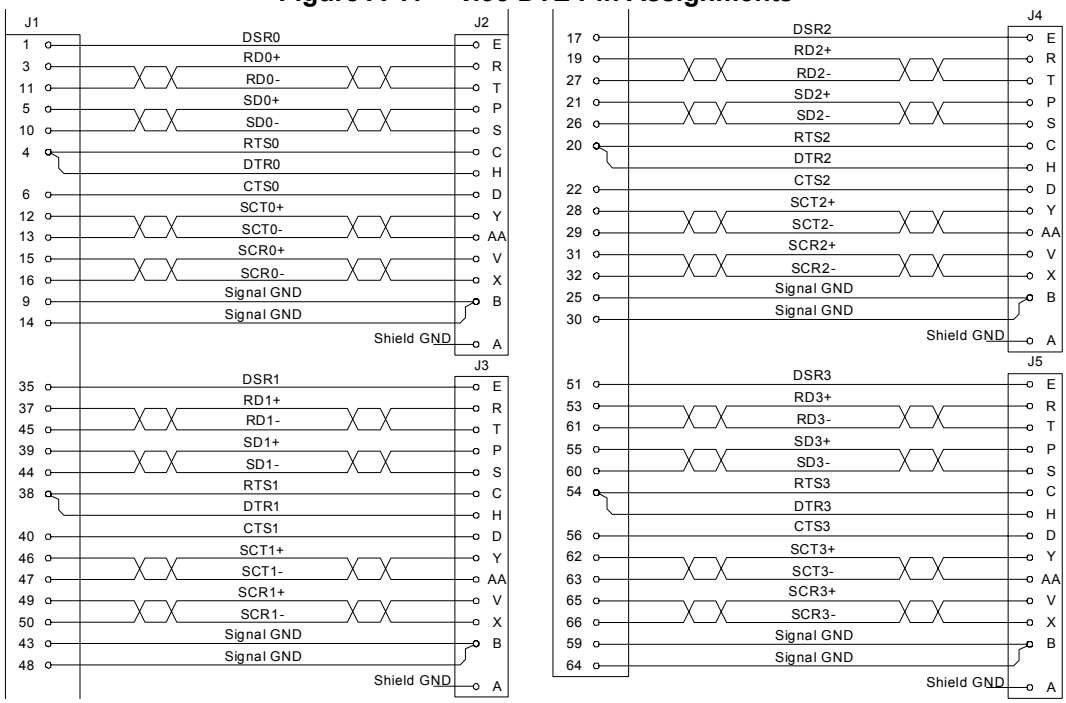
J1: 68-pin male SCSI II type connector
J2 - J5: DB-37 type male connector

Figure A-10 Combined V.35/EIA-232/530 DTE Pin Assignments



J1: 68-pin male SCSI III-type connector
J3, J5: V.35-type male connector
J2. J4: DB-25-type male connector
Pins not shown are unused.

Figure A-11 V.35 DTE Pin Assignments



J1: 68-pin male SCSI II type connector
J2 - J5: V.35 type male connector

T1/E1/ISDN PRI NIM Card Ports

The T1/E1/ISDN PRI NIM comes equipped with either 1, 2 or 4 Ethernet (WAN) ports that support fractional T1/E1 transmission in full-channel, fractional or unchannelized format with 8-pin modular RJ-48C connectors and include a built-in DSU/CSU, as shown in Figure A-12.

Cables required for these ports must be 100-ohm, straight-through, twisted-pair for T1 lines and a 120-ohm version for E1 lines. Refer to Figure A-13 for pinout assignments.

Note: m version for E1 lines. Refer to Figure 13 for pinout assignments. If you are using the TI/EI/ISDN PRI NIM in Singapore or Australia, the cables required for these ports must not employ individual shields for each pair.

Figure A-12 4-Port T1/E1/ISDN PRI NIM Card (RJ-48C ports shown)

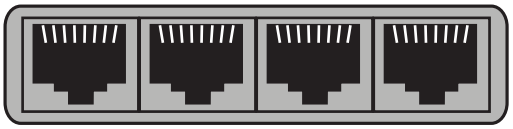
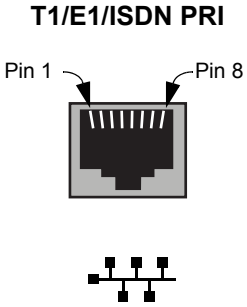


Figure A-13 T1/E1 NIM Port Pinouts



Pin	Signal
1	Receive Ring
2	Receive Tip
3	Chassis GND (optional)
4	Transmit Ring
5	Transmit Tip
6	Chassis GND (optional)
7	no connection
8	no connection

Regulatory/Safety Compliance

The T1/E1 ISDN PRI NIM complies with these regulatory requirements: PCI Local Bus Specification Rev 2.1, IEEE P1386 Draft 2.4, IEEE P1386.1 Draft 2.4, ANSI T1.403, ITU-T G.703, G.704, G.706, G.736, G.775, G.823, I.431, Q.703, AT&T TR62411 and TR54016, ETSI ETS 300233, and IEEE 1149.1.

The NIM also complies with the following safety requirements: CS03, FCC Class B, TBR12-14, GR-1089, ITU K17-K20, IEC 61000-4-2, IEC 61000-4-5, UL 1950, IEC 950, and EN 60950.

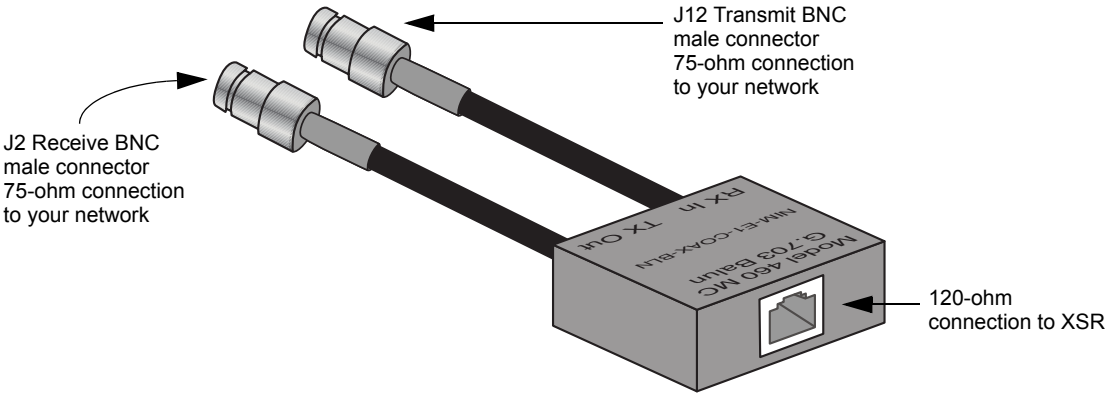
Balun for E1 or PRI NIM Cards

Some overseas electrical systems require that you use a balun and grounding shunt when utilizing an E1 or PRI NIM card on the XSR. A balun is an adapter employed to connect a 75-ohm coaxial cable pair (2 BNC connectors) to a 120-ohm twisted pair cable (RJ-48C connector).

The balun and its connectors are shown in Figure A-14. The grounding shunt is also required to insulate (ground) unused pins of the RJ-48C connector.

To install the balun, attach the 75-ohm coaxial cables to the BNC connectors and a 120-ohm E1/PRI cable to the RJ-48C port (see below for details).

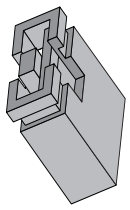
Figure A-14 Balun for E1 or PRI Connection



Grounding Shunt for E1 NIM Cards

If you connect a balun to a 75-ohm line, you will also need to attach a grounding shunt (or terminal strip) to any NIM pins whose RJ-48C connectors utilize the balun. The XSR requires that you use a shunt (shown in Figure A-15), or terminal strip to ground pins 3 and 6 of the RJ-48C interface, which are not needed to complete the connection.

Figure A-15 Sample Grounding Shunt



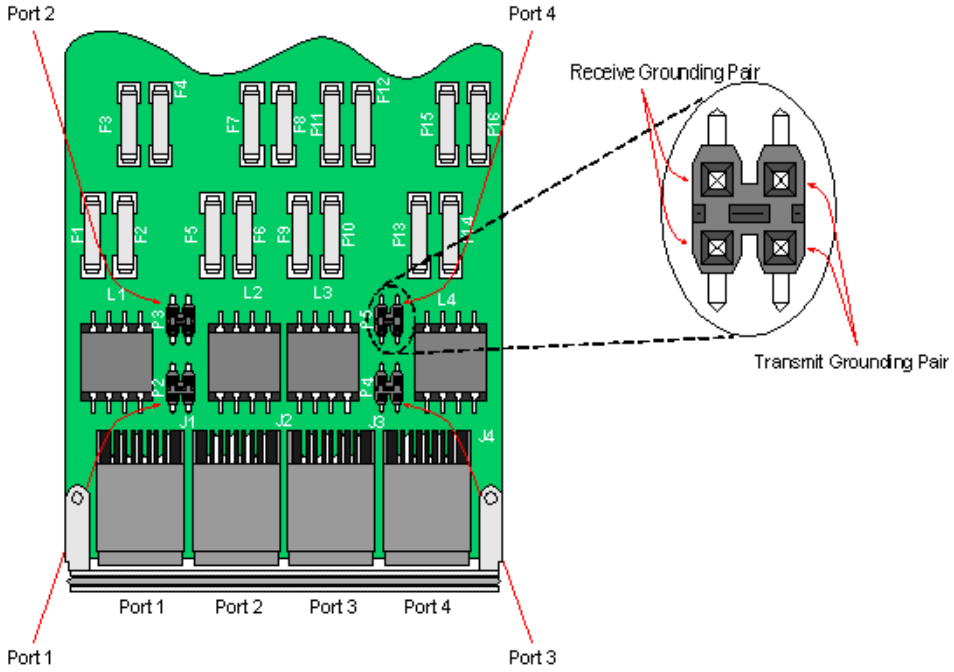
Caution: The cable connecting the E1/ISDN PRI NIM to the balun requires two more wires to extend the chassis ground to the balun. Cables of this type are often provided by your supplier who can customize them to your needs.

Refer to *"Hardware Installation" on page 2-1* to access the E1 card on the XSR.

Installing Shunt/Terminal Strip

To install the shunt or terminal strip, attach two dual-pin units vertically to each four-pin jumper (P2, P3, P4, or P5) corresponding to the RJ-48C port using a balun, as shown in Figure A-16. Any other RJ-48C ports on the NIM card connected to 120-ohm lines do not require shunts.

Figure A-16 Installing a Grounding Shunt on the E1 NIM Card



T3/E3 NIM Card

The T3/E3 full and sub-rate NIM, as shown in Figure A-17, is equipped with 1 Ethernet (WAN) port that supports fractional T3/E3 transmission in un-channelized or clear channel mode with BNC connectors. User data are encapsulated in HDLC packets before being sent to the line.

Figure A-17 1-Port T3/E3 NIM Card

Cables required for this NIM must be 75-ohm, DS3 Type 734 or 735 coaxial. DS3 cables support a length up to 450 in length. E3 cabling supports a cable length up to 900 feet.

Un-channelized mode consists of the entire T3/E3 payload in one data path, but with T3/E3 framing bits still in place. Only one HDLC channel is used. Throughput of the un-channelized link can be limited by using only a portion of the entire payload. Various sub-rates are available to provide compatibility with major DSU equipment suppliers. Scrambling may also be enabled as required for DSU compatibility. Larscom zero suppression is supported.

Clear channel mode presents the board merely as the line driver for a link carrying HDLC packets where even framing bits are used for data transfer. The T3/E3 framer operates in bypass mode and renders the NIM a line driver. Both sides of the link must have the same setting to operate correctly in this mode.

For more details on software configuration, refer to the *XSR User's Guide*.

Regulatory/Safety Compliance

The T3/E3 NIM complies with the following regulatory requirements.

E3: FCC Class B, ITU-T G.703, G.704, G823 and TBR24 for world wide approval, National Standards testing as required, and BABT Compliance United Kingdom directive 607114.

T3: FCC Class B, GR-499-CORE is the Bellcore test procedure that can be used for design validation, JATE Green Book for Japan.

1/2-Port BRI-S/T NIM Card Ports

The XSR offers a serial NIM card for 1 or 2 WAN interfaces over an ISDN-S/T BRI line, as shown in Figure A-18. Port 0 and 1 LEDs shine when the lines are active and ready to receive traffic. Refer to Figure A-19 for pinout assignments.

Figure A-18 ISDN BRI-S/T NIM Card (RJ-45 ports shown)

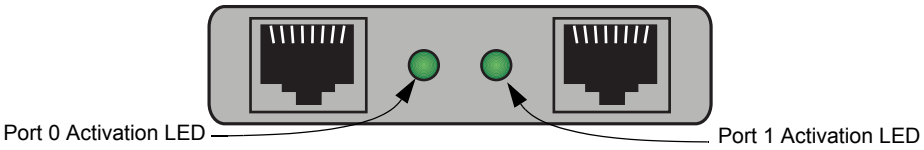
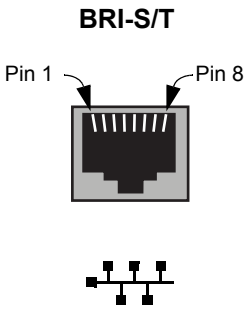


Figure A-19 ISDN BRI-S/T -NIM Pinouts



Pin	Signal
1	Unused
2	Unused
3	Transmit (+)
4	Receive (+)
5	Receive (-)
6	Transmit (-)
7	Unused
8	Unused

Termination Shunt for the ISDN BRI-S/T NIM Card

ISDN BRI-S/T terminal equipment devices may be connected at random points of the cable in point-to-point or point-to-multipoint configurations. Line termination resistors must be provided at both ends of the transmit/receive lines only.

The XSR's BRI NIM card provides an option to terminate receive as well as transmit lines using 100 Ohm resistors. Shunts are required to shorten the appropriate contacts of the terminal headers (P1, P2). Refer to "Installing Shunt/Terminal Strip" on page A-17 for directions.

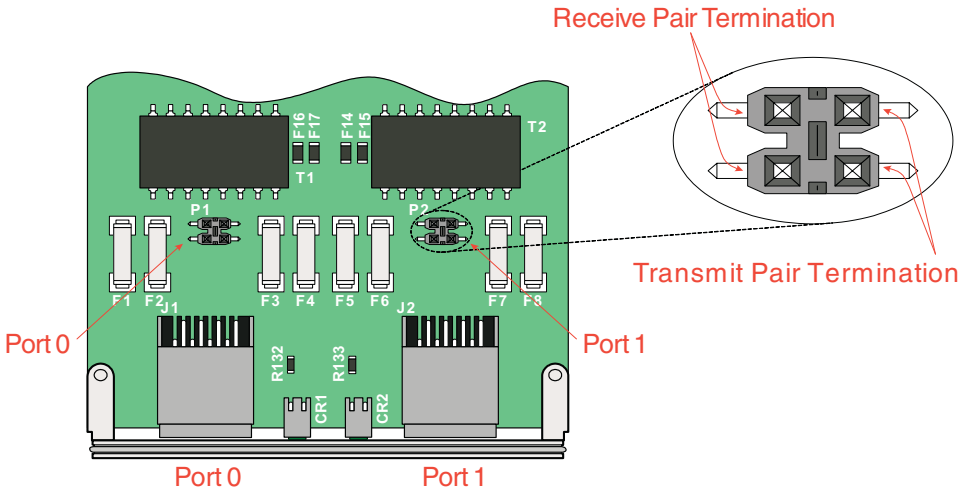
Figure A-20 below shows per port respective termination header locations and the orientation of the receive and transmit pairs.

Caution: The cable connecting the BRI NIM to the balun requires two additional wires to extend the chassis ground to the balun. Cables of this type are often provided by your supplier who can customize them for your needs.

Installing Shunt/Terminal Strip

To install the shunt or terminal strip, attach two dual-pin units vertically to P1 and P2 four-pin jumpers corresponding to the RJ-45 port using a balun, as shown in Figure A-20. Any other RJ-45 ports on the NIM card connected to 120-ohm lines do not require shunts.

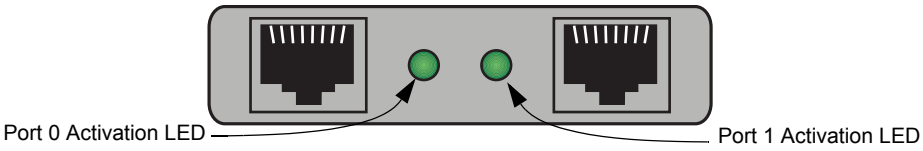
Figure A-20 Installing a Termination Shunt on BRI-S/T NIM Card



1/2-Port BRI-U NIM Card Ports

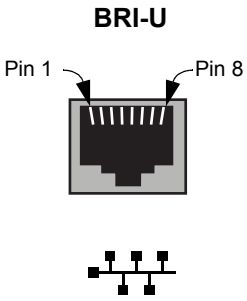
The XSR provides a serial NIM card for 1 or 2 WAN interfaces over an ISDN BRI-U line, as shown in Figure A-21. The Port 0 and 1 LEDs shine when the lines are active and ready to receive traffic.

Figure A-21 ISDN BRI-U NIM Card (RJ-49C ports shown)



Refer to Figure A-22 for pinout assignments.

Figure A-22 ISDN BRI-U -NIM Pinouts



Pin	Signal
1	Unused
2	Unused
3	Unused
4	Signal (Tip)
5	Signal (Ring)
6	Unused
7	Unused
8	Unused

Regulatory/Safety Compliance

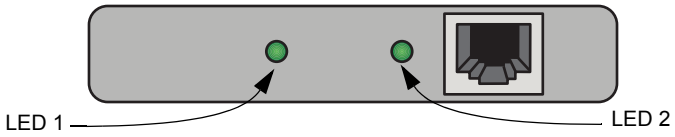
The ISDN BRI-U NIM complies with the following regulatory requirements: PCI Local Bus Specification Rev 2.2, IEEE P1386 Draft Rev 2.4, IEEE P1386.1 Draft Rev 2.4, ANSI T1.601-1999, and IEEE 1149.1.

The NIM also complies with the following safety requirements: FCC Part 68, CS03, FCC Class B, UL 1950, IEC 950, and EN 60950.

1-Port ADSL NIM Card Port

The XSR's Asymmetric Digital Subscriber Line (ADSL) NIM card, as shown in Figure A-23, provides 1 WAN port on an ADSL over POTS (Annex A/C) or ISDN (Annex B) line with a 6-pin RJ-11 connector. The ADSL NIM supports both G.dmt and G.lite standards. ADSL NIMs are shipped with a CompactFlash card containing DSP firmware. This driver software copies the Flash file into host memory where it provides on-demand use by the DSP.

Figure A-23 ADSL NIM Card



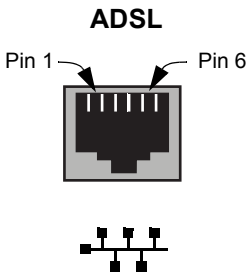
Note: The XSR supports only one ADSL card type at a time, so multiply-installed card types must be similar.

The XSR supports only one ADSL card type at a time, so multiply-installed card types must be similar.

The LEDs behave as follows: LED 1 - *Status* - When OFF, the line is down; when ON; the line has ended "training" or synchronization with the remote DSLAM device and is operational; when Flashing, the line is in training mode; LED 2 - *Data* - When flashing, traffic is active.

Refer to Figure A-24 for pinout assignments.

Figure A-24 ADSL NIM Pinouts



Pin	Signal
1	Unused
2	Unused
3	Signal (Tip)
4	Signal (Ring)
5	Unused
6	Unused

Regulatory/Safety Compliance

The ADSL NIM complies with these regulatory requirements: EN 55022, EN 55024, FCC Part 68, CS03, TIA/EIA-IS-968, T1.413, ITU G.992.1, ITU G.992.2, ITU G.991.2, ITU G.994.1, Deutsche Telecom U-R2 specifications and ANSI Standard T1.413-1998 (issue 2) specifying full rate ADSL.

The ADSL NIM also complies with the following safety requirements: UL 1950, CSA No. 950, EN 60950, and IEC 950 (CB Scheme Report).

T1/E1 Drop & Insert (D&I) NIM

The XSR's 2-port T1/E1 D&I NIM card, as shown in Figure A-25, is designed as an intermediary between the Central Office T1/E1 line and a PBX. It de-couples Channel Associated Signaling (CAS) and Voice DS0 timeslots and redirects them to a PBX, and conversely, reintegrates Voice DS0 timeslots from the PBX with the T1/E1 data stream. Both ports are functionally equivalent.

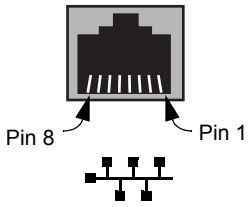
Figure A-25 T1/E1 D&I NIM Card

The T1/E1 D&I NIM provides long- and short-haul capabilities and Drop and Insert functionality via a fully configurable Time Division Multiplexed (TDM) switch. It can be configured for data only, or voice/data applications. In Data-Only mode, both ports pass data, whereas in Voice/Data mode, one port passes a voice/data stream, while the other passes only voice.

The T1/E1 D&I NIM maintains high reliability of voice traffic by using a bypass relay to ensure continued service even if a power failure occurs or the NIM enters an abnormal state. In such an event, the two ports are connected, bypassing the NIM, thus allowing uninterrupted bidirectional voice transmission. To ensure service, remember to configure voice timeslots on both sides of the connection in the same manner. That is, if timeslots 3-5 are configured for voice on the NIM, the same DS0s should be configured for voice at the Central Office. Refer to the *XSR User's Guide* for instructions.

Refer to Figure A-26 for pinout assignments.

Figure A-26 T1/E1 D&I NIM Pinouts



Pin	Signal
1	Unused
2	Unused
3	Unused
4	Signal (Tip)
5	Signal (Ring)
6	Unused
7	Unused
8	Unused

Regulatory/Safety Compliance

The T1/E1 D&I NIM complies with the following regulatory requirements: PCI Local Bus Specification Rev 2.1, IEEE P1386 Draft 2.4, IEEE P1386.1 Draft 2.4, ANSI T1.403, ITU-T G.703, G.704, G.706, G.736, G.775, G.823, I.431, Q.703, AT&T TR62411, TR54016, ETSI ETS 300233, and IEEE 1149.1.

The T1/E1 D&I NIM also complies with the following safety requirements: FCC Part 68, CS03, FCC Class B, TBR12, 13, 14, GR-1089, ITU K17-K20, IEC 61000-4-2, IEC 61000-4-5, UL1950, IEC 950, and EN 60950.

CompactFlash Memory Card

The optional plug-in CompactFlash (CF) memory card, shown in Figure A-27, comprises a single chip controller and flash memory modules in a matchbook-sized package with a 50-pin, PCMCIA connector consisting of two rows of 25 female contacts each.

The PCMCIA male interface supports both Type I and Type II CF cards. Note that the CF release mechanism pops out when you install the card. For installation instruction, refer to “Hardware Installation” on page -1.

Figure A-27 CompactFlash Memory Card

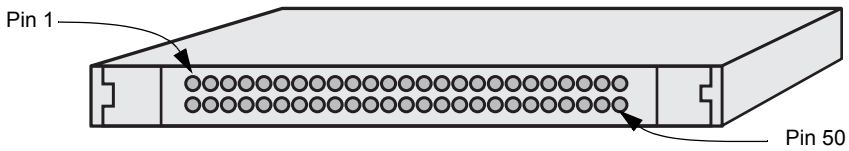


Figure 1 CompactFlash Memory Card

LED Behavior

The 14 LEDs on the XSR front panel display system and port status as described in Table A-3. The six system LEDs are illustrated to the left and the eight GigabitEthernet LEDs to the right in Figure A-28. Note that Link and TX (transmit) green LEDs are provided for the GBIC port while each GigabitEthernet port has one green and one amber LED.

Figure A-28 XSR LEDs

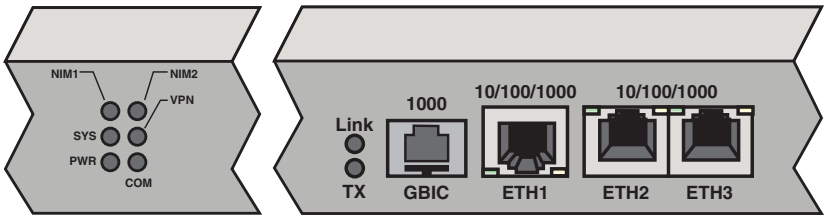


Table A-3 LED Description

LED	State	Function
NIM 1, NIM 2	ON	T1/E1, ISDN or HSSI card is present and power-up diagnostics test passed
	OFF	NIM slot empty or power-up diagnostics test failed
SYS(tem Status)	ON	XSR is operational
	OFF	Faulty hardware or Bootprom
	Blinking	Flash update is in progress (software image downloading), warning you not to power down the XSR. Powering down now can leave the branch router without valid software.

Table A-3 LED Description (continued)

LED	State	Function
PWR	ON	XSR is powered up and Bootrom initialized
	OFF	XSR is powered down
VPN	ON/OFF	VPN tunnel is up/No tunnel connected
COM(munication)	Blinking/OFF	Port is transmitting or receiving data/idle
Ethernet Port 1, 2, 3	Amber only ON	10Base-T link is auto-detected
	Green only ON	100Base-T link is auto-detected
	Both ON	1000Base-T link is auto-detected
	Blinking	Port is transmitting or receiving data
	OFF	Link is down
Fiber/Copper Mini-GBIC (Ethernet) Port	Both OFF	Port is configured as copper
	Link LED ON	Fiber link up
	TX LED Blinking	Activity on fiber port
BRI NIM Port 0/1	Connected to switch	BRI link is activated and ready for traffic. This LED is located on the NIM card.
ADSL NIM 1	Blinking	Line is in training mode (syncing with DSLAM)
	ON	Training mode complete, line is operational
	OFF	Line is down
ADSL NIM 2	Blinking	Traffic activity in sync with data traffic
T3/E3 NIM: •LOS (Loss of Signal) •LOF (Loss of Frame) •Alarm •Enable	 Red ON Red ON Amber ON Green ON	 XSR cannot latch onto the frequency Both sides of link cannot synchronize frames Error condition detected Link is up and running
Copper Ethernet NIM	Link ON Link OFF Activity Blinking	100Base-T link is auto-detected 10Base-T link is auto-detected Port is transmitting or receiving data
Fiber-optic Ethernet NIM	Link ON Activity ON	100Base-F link is auto-detected Port is transmitting or receiving data

Index